An Coimisinéir Cosanta Sonraí

Data Protection Commissioner

Annual Report

of the
Data Protection Commissioner
2007

Presented to each of the Houses of the Oireachtas pursuant to section 14 of the Data Protection Acts 1988 & 2003.

PRN. A8/0298

30-01 04/08 (800) Brunswick Press Ltd. (20576)

Contents

Foreword

In this, my third year as Commissioner, perhaps it would be easy to adopt a congratulatory approach in relation to what has been achieved over the past year. We have seen a rise in knowledge and awareness generally of data protection rights and obligations. This is evidenced by the growth in the numbers of complaints which my Office is receiving, the numbers of queries we are fielding, the number of data breach reports being made by data controllers and the significant media interest in privacy and data protection issues generally.

In many respects this represents the mainstreaming of data protection into the operations and functions of public bodies and private organisations and in the public consciousness generally. Naturally, I very much welcome this trend. However, any temptation towards complacency was quickly dispelled as attention focussed on how the State protects the personal data that we entrusted to it. To some degree, this focus was a result of the astonishing loss of personal data relating to a large proportion of the population of the UK. The existence of similar risks in this jurisdiction was confirmed by revelations about unauthorised access to personal data held by some of our own public bodies.

In a previous Annual Report I quoted a colleague's description of privacy as being in "a cold place". Against an international background of curtailment of civil liberties, I was concerned that the individual's right to privacy might be sacrificed unnecessarily in pursuit of a security agenda or for the sake of greater efficiency in the provision of public services.

Security issues are still setting the public agenda to a large extent. Have we not succumbed to terror and submitted to extremism when we lose the liberty to live our lives without constant intrusion by the State in the name of security? When I consider the security measures introduced in this jurisdiction, it is sometimes difficult to avoid the conclusion that Ireland must be facing some of the starkest criminal and terrorist threats across Europe. The three-year retention regime for telecommunications data is just one example of a trend that includes the innocuously titled e-borders system and extensive proposals in relation to a DNA database. These initiatives, discussed elsewhere in this report, will further erode our civil liberties if they are introduced without appropriate safeguards for the privacy of law abiding citizens. I remain hopeful that, through dialogue, the State can pursue its legitimate security agenda without unnecessarily and systematically intruding into each of our personal lives.

Recognising the reality of these threats to our privacy, the staff of my Office have undertaken a new initiative of their own. This year, and for the first time, they have put together a list of the top threats to privacy based on the issues which they have encountered over the past year. There is nothing scientific or authoritative about this list; instead, we intend it to provoke discussion. We intend to repeat the exercise each year as a kind of barometer of privacy concerns. I hope that the list gets shorter!

Finally, I would like to record my appreciation to the staff of the Office for the immense dedication and effort which they have demonstrated over the past year. They have shown integrity and flexibility in dealing effectively and professionally with the vast array of issues which my Office is called upon to deal with.

Billy Hawkes
Data Protection Commissioner
Portarlington, March 2008

Top Ten Threats to Privacy

As mentioned above, we have decided to publish the top ten threats to individual privacy as identified by our staff. This unscientific list represents our perception of the issues at the close of 2007; each year, we will renew the list and our rankings to identify the biggest risks of that particular year.

1. Lack of proper procedures in public and private sector bodies to limit access by their employees to our personal data on a 'need to know' basis.

2. The interaction of the security agenda with our everyday lives as evidenced by increasing requirements for us to hand over our data and for those holding it to keep it and give it to law enforcement when required to do so.

3. The extended use of the Personal Public Service Number (PPSN). This is the number given to each one of us by the Government to identify us during certain interactions with public bodies. More and more services are seeking to use this identifying number and plans are afoot to require the private sector to collect it for certain transactions with all of us also. It therefore becomes easier for databases to be linked together.

4. Excessive personal data being sought in the context of international travel.

5. The collection and retention of excessive amounts of personal data. Data controllers need to seek and retain only what they really need to perform a service or task.

6. Publication and availability of personal data on the internet (sometimes placed there by the individuals themselves on social networking sites etc).

7. The exploitation of mobile phone numbers for marketing purposes.

8. The increasing and unthinking use of biometrics in the workplace (and even in schools).

9. Continued lack of awareness among data controllers of their data protection obligations.

10. Continued lack of awareness and complacency on the part of members of the general public - giving away our personal information too easily, not asking why the information is needed or ticking the box to say that we don't want to be contacted. I will continue to work hard to improve this position.

PART 1 - ACTIVITIES IN 2007

Introduction

Any perception that 2007 might prove to be a year of quiet consolidation for my Office after its successful decentralisation to Portarlington in December 2006 was quickly dispelled during the course of the year. There is a significantly increased focus on privacy and data protection issues amongst the public, the media and, in turn, amongst those entities holding our personal data.

Real measurements of public awareness of data protection issues can be hard to pin down but the substantial increase in the number of complaints received by my Office each year is a useful indicator. In 2005 we received 300 complaints alleging breaches of data protection legislation. In 2006 that figure increased to 658. In 2007, the number of complaints received by my office reached 1037. These figures only include complaints that needed to be formally investigated. Many other complaints were resolved through our help-desk without requiring such investigation. We have sought as an Office to enthusiastically respond to this increased focus on the role and requirements of the Data Protection Acts.

The responsibility of Government to safeguard personal information entrusted to it by members of the public has been an important focus of my Office throughout 2007 and into 2008. There is often a legal requirement for members of the public to hand over their personal information to public bodies. Any failure by public bodies to keep this information secure is therefore all the more serious. Regrettably, 2007 saw a number of reports of improper access by civil servants to personal information entrusted to their departments. There were also reports of deliberate improper release of personal information to third parties. While those who betray the public trust in this way must be punished appropriately, the best protection for the public is to limit access to the information in the first place and to audit that access subsequently. Given the amount of public attention to data protection issues, public bodies can expect their security systems to be increasingly subjected to public scrutiny.

Unfortunately over the past year we have also seen abundant evidence of poor standards of protection of customers' personal information in the private sector. Companies that hold large volumes of personal or sensitive data, such as those in the financial and insurance sector, are particularly vulnerable. Recent examples of accidental disclosure of customer information in the private sector have included sensitive personal data related to health and financial status. The disclosures have typically come about through inadequate security procedures, low standards of staff training and a failure to take data protection considerations into account when business systems were originally devised. While companies in the financial, insurance or service sector may be particularly vulnerable to accidental loss of customer information, any company that holds information on customers or employees can find itself compromised by data disclosure. The reputational damage that results can have deeply unpleasant consequences for a company in terms of customer confidence, legal action and employee relations.

To ensure the highest standards of protection for the personal data of members of the public, private companies and public bodies must ensure that security

and privacy specifications are incorporated into the design of large information systems. It is very difficult and expensive to graft data protection elements onto existing systems. It is also essential that organisations incorporate data protection into their induction and training systems. Employees must understand their duty to protect the confidentiality of personal information. Finally, organisations (particularly those holding large quantities of personal data or particularly sensitive personal data) should pro-actively audit access to personal data to detect any irregular patterns of access or use of the data by employees. No system is perfect, but I expect organisations to take their data protection responsibilities seriously, with adequate security arrangements, a coherent data protection policy, clear audit arrangements and plans in place for reacting to security breaches.

Customer Service and the Provision of Information & Advice

The core mission of the Office of the Data Protection Commissioner is the protection of the individual's right to privacy by enabling people to know, and to exercise control over, how their personal information is used. Accordingly my Office maintains a strong focus on the provision of comprehensive, accurate and practical advice on data protection for all our customers, whether they are the people about whom data is held (data subjects) or the entities holding that data (data controllers). Over the past year our helpdesk has responded to approximately 20,000 phone enquiries, together with over 4,000 email enquiries and a smaller number of contacts by post. This large number of queries is partly a result of effective education and awareness-raising exercises and increasing numbers of audits and inspections. However it also reflects the strong and very valuable media profile built up by the Office of the Data Protection Commissioner as journalists engage with privacy issues as a matter of major public concern.

All staff of the Office of the Data Protection Commissioner are involved in the provision of advice and information directly to our customers (our customers include both data subjects and data controllers). This reflects our belief that direct communication with our customers is the best means of ensuring that we keep our advice current and relevant. As part of this broad effort we have completed a comprehensive update and expansion of the information on our website (including a new Frequently Asked Questions section) and we are currently developing a new layout to increase the accessibility of this key customer information resource. We are continuing to investigate innovative media channels as awareness raising tools. For example, at the start of 2008 we launched a new privacy competition on YouTube.

During 2007 the staff of the Office and I made 59 presentations to various sectors and organisations (see appendix 1) in comparison with 35 presentations in 2006. We try to accept as many appropriate invitations as possible to make presentations to data controllers[1] (in both the public and the private sectors) about their data protection obligations. These presentations are an important opportunity to interact with data controllers about their data protection obligations and about privacy issues more generally. Such issues

1 "data controllers" are organisations that collect and hold personal data on individuals ("data subjects")

include the privacy implications of new technologies and the challenges facing businesses as they try to act responsibly in relation to personal data. We also make presentations to groups concerned with the rights of data subjects, raising awareness of data protection rights and the steps that can be taken to defend these rights.

Business Plan Report

Our Business Plan for 2007 was focused on the provision of comprehensive, definitive and clear information to the public on data protection issues and on improving awareness among data subjects and controllers of their rights and obligations. Key elements of our efforts to fulfil these objectives included effective awareness raising exercises; increasing numbers of audits and inspections; our valuable media profile; and further development of our website as a key customer interface. The strong commitment of my staff to responding to customer queries quickly and accurately is an important strength of my Office (as far as possible they respond on the day of receipt). My staff are maximising the potential of new technology through further development of our website, in pursuit of a 24/7 service by the Office. This performance means that the key objectives set out in our Business Plan for 2007 have been substantially achieved and we are now focused on our key objectives for 2008 as set out in our new Business Plan.

Irish Language Scheme

In July 2006, my Office invited submissions in relation to the preparation of an Irish Language Scheme for the Office under the Official Languages Act 2003. We prepared the Scheme taking into account five submissions received from interested parties. It can be viewed at *www.dataprotection.ie.* The Scheme outlines the services provided by the Office through the medium of Irish and the measures to be taken to develop these services further, including through building on the language skills of our staff. We are fully committed to meeting each of the commitments outlined. The Scheme was confirmed by the Minister for Community, Rural & Gaeltacht Affairs and took effect from 1 April 2007 for a period of three years.

Cooperation with other Government Bodies and Agencies

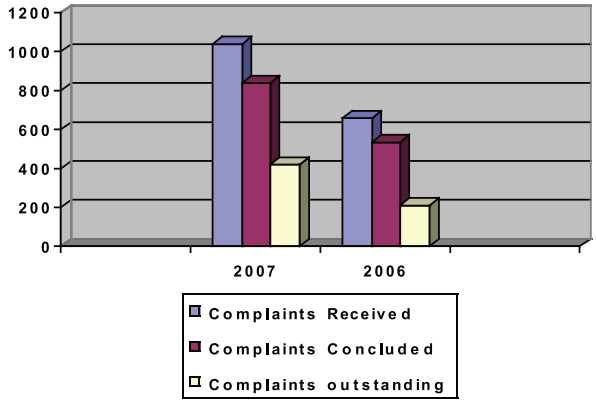
Data Protection does not, of course, exist in isolation and, as a relatively small Office, it would not be possible for us to fulfil our mandate effectively without the cooperation and assistance of a number of other bodies and agencies. Recognising the value of this cooperation, we continue to maintain excellent relations with the Irish Human Rights Commission, the National Consumer Agency, the Commission for Communications Regulation (ComReg), the Independent Regulator of Premium Rate Telecommunications Services (RegTel), the Director of Corporate Enforcement, An Garda Síochána,

COMPLAINTS AND INVESTIGATIONS

the Companies Registration Office, the Financial Regulator, the Financial Services Ombudsman, the Internet Advisory Board, the Health Service Executive, the Health Information and Quality Authority and a number of other partner bodies.

The number of new complaints received during the year was 1,037 (compared to 658 in 2006 and 300 in 2005). By any standards, this represents a significant increase in the workload of my Office's Investigation Unit over the past couple of years. Similar to last year, the biggest factor in the increase was the significant number of complaints which fall under the Privacy in Electronic Communications Regulation (S.I. No. 535 of 2003). 538 such complaints (relating to unsolicited text messages, phone-calls and emails) were dealt with in 2007 compared to 264 in 2006 and 66 in 2005.

Figure 1: Complaints Received, Concluded and Outstanding



One of the main contributory factors to the increase in complaints under S.I. 535 of 2003 was the greater level of public awareness which emerged during the year concerning, in particular, unsolicited marketing text messages. There was substantial media coverage concerning the infringement of the data protection rights of mobile phone users which, in turn, led to complaints to my Office from affected members of the public. In particular, the airing by RTE television of a Prime Time feature on this subject in February, and follow-up debate and discussion through other

media outlets, raised awareness significantly and prompted large number of mobile phone subscribers to report their own experiences to my Office. I very much welcome the role that the media has played in highlighting this issue and in creating a greater awareness among mobile phone users of their rights in this area.

Figure 2: Breakdown of Complaint by Data Protection issue

Direct Marketing	5%
SI535	52%
Access Rights	18%
Disclosure	10%
Accuracy	2%
Other	13%

Figure 3: Complaints received since 2000

Year	Complaints Received
2000	131
2001	233
2002	189
2003	258
2004	385
2005	300
2006	658
2007	1037

When a complaint is received, I am required by section 10 of the Acts to investigate it and to try, in the first instance, to arrange an amicable resolution. In 2007 my Office made significant efforts to arrange amicable resolutions of complaints by the fastest possible means.

In many cases an admission by a data controller that they have breached the Acts, with an apology to the data subject concerned, is sufficient to satisfy the data subject and to amicably resolve the complaint. In other cases a goodwill gesture by the data controller to the data subject, in addition to an apology and an admission of wrongdoing, may help to satisfy the data subject. My Office has negotiated several goodwill gestures on behalf of data subjects during the year. Such goodwill gestures might involve, for example, a gift token for the data subject or a donation to a charity of the data subject's choice. Thankfully the vast majority of complaints are resolved without it being necessary for me to issue a formal decision under Section 10 of the Acts.[2]

As Commissioner, I do not have power to award compensation. However, if a data controller fails to observe their duty of care in respect of personal data, they are liable to be pursued for damages through the courts (under Section 7 of the Acts). My Office has no function in relation to any such proceedings.

Access Rights

In last year's Annual Report, I referred to a radical change in my Office's approach to resolving complaints from data subjects concerning access requests. I indicated that our emphasis now is on enforcement. This reflects my view that the right of access is at the heart of data protection rights; at the most fundamental level, it enables people to know what personal data is being held about them and, therefore, to begin to exercise control over how that data is used.

2 In 2007 I made a total of ten formal decisions, two of which rejected the substance of the data subject's complaint.

I am pleased to report that our new approach has been a significant success and has yielded positive results for the complainants concerned.

Failure to respond to an access request within the forty-day timeframe provided under the Acts results in a breach of a data subject's right of access. In addition, a data controller who fails to inform the data subject of the reason for refusing an access request contravenes Section 4(7) of the Acts. Under our procedures, data controllers who appear to be breaking the law in this way are given ten days from the start of my investigation to inform the data subject in writing (and to copy the correspondence to my Office) of the provisions of the Acts upon which it is relying to withhold the personal data. If the data controller is unable to refer to any such provisions, it must comply with the access request immediately or I will bring my Office's legal powers to bear on the case without further notice.

In the course of 2007, my Office processed 83 complaints under this new procedure. The vast majority of data controllers who were investigated in relation to these complaints responded to my Office and took immediate steps to fulfil their obligations to comply with the data subject's request.

The right of individuals to access their personal data also benefited from the publication by the Department of Finance in December 2006 of a new guidance notice (Central Policy Unit – Notice No. 23) on Data Protection and Freedom of Information (FoI) in the Public Sector. The Notice set out to outline the provisions governing rights of access to personal information under the Freedom of Information and Data Protection Acts.

It also described the procedural arrangements which public bodies should follow when dealing with requests for access by individuals to their own personal information under those Acts. The Notice outlined the following procedures:

- When a public body receives a request from, or on behalf of, a person seeking access to their own personal information under the FoI Act, this request should also be taken as a request under the Data Protection Acts. This is because a valid data protection access request does not need to refer to the Data Protection Act.
- If a public body considers that the release of information is exempt under one Act, their possible release under the other Act should be considered as a separate exercise. So, for example, if a body is considering refusal of access under the FoI Act, it should check that such refusal is permitted under the Data Protection Acts and vice versa.
- A decision on the request should be issued within the most favourable time-scale provided for by law (usually the timescale under FoI).
- If the decision is taken to refuse access by an individual to some or all of her/his personal information, the decision letter should refer to the individual's right to internal review under the FoI Acts and to the right to complain to the Data Protection Commissioner under the Data Protection Acts.

Use of Full Legal Powers

As I have stated above, thankfully it is possible to conclude the vast majority of complaints to my Office in a swift and amicable manner with the assistance of all involved. Unfortunately, this is not always the case and where I find that an investigation is being unreasonably stymied, I have no hesitation in using the full legal powers available to me. This year I am including for the first time a list of those occasions where I have had to resort to the use of my legal powers to advance an investigation. I hope that this will serve to encourage all organisations to fully co-operate with my Office in relation to our legitimate investigations. Over the past year, I have also noted instances where the involvement of solicitors acting for data controllers has sometimes led to confusion and delay in finalising complaints. This has been particularly notable in a number of cases involving access requests to schools. I fully respect the right of any person or entity to engage legal assistance in responding to queries from my Office. Such assistance can help data controllers to better understand their obligations under data protection legislation and to put in place procedures to ensure that these obligations are met. However, where solicitors are retained, I will not accept lengthy periods for deliberation of legal issues or the establishment of facts which are abundantly clear. If, in future, I find that solicitors are behaving in a manner that obstructs my Office in the discharge of its statutory duties, I will consider naming the firms in question in my Annual Report.

Enforcement Notices[3] Issued in 2007

Data Controller	In relation to
Insight Investigations	Section 4 (1) of the Data Protection Acts
Insight Investigations	Section 4 (1) of the Data Protection Acts
Mr. Mark Doyle, Freelance Photographer	Section 4 (1) of the Data Protection Acts

Selected Information Notices[4] Issued in 2007

Data Controller
Frank Buttimer & Co. Solicitors on behalf of a client
Meagher Solicitors on behalf of a client
The Manager, Manulla National School
Iarnród Éireann
Sunday Newspapers Ltd T/A The Sunday World

3 Under section 10 of the Data Protection Acts, 1988 and 2003, the Data Protection Commissioner may require a data controller or data processor to take whatever steps the Commissioner considers appropriate to comply with the terms of Acts.

4 Under section 12 of the Data Protection Acts, 1988 and 2003, the Data Protection Commissioner may require any person to provide him with whatever information the Commissioner needs to carry out his functions, such as to pursue an investigation. The Information Notices listed here do not include Notices issued in circumstances where the data controller might otherwise have felt unable to supply information due to confidentiality obligations.

Unsolicited SMS Messages

Last year, I reported that the number of complaints to my Office relating to unsolicited SMS messages was growing. I indicated that I would use my full powers in 2007 to ensure that the text marketing sector fully understand their data protection obligations. As I have outlined above, the number of complaints regarding unsolicited text messages increased in 2007 to a total of 390 (representing 38% of complaints overall).

During the year, my Office undertook a number of initiatives:

- Early in 2007 my Office published a substantial guidance note on the use of electronic mail for direct marketing purposes to assist individual subscribers and for persons engaged in direct marketing activity. The guidance material is entitled 'Dealing with Unsolicited Commercial Communication (SPAM)' and is available at www.dataprotection.ie
- In conjunction with the Regulator of Premium Rate Telecommunications Services (RegTel), my Office initiated high level contact with all four mobile telecommunications operators, Meteor, O2, 3 and Vodafone. Following a very positive engagement, a common understanding was reached regarding how we could cooperate in the interests of consumers under the current regulatory framework. This common understanding included, amongst other things, measures to exchange relevant information in respect of the investigation of offences. It also provided for efforts to ensure that premium rate text messages carried by the mobile network operators on behalf of service providers have the prior consent of subscribers.
- In the summer of 2007, my Office undertook 'raids' of a number of companies engaged in the mobile text marketing sector. These snap inspections came in response to the large number of complaints received in my Office in relation to those companies and as part of my strategy to use my full powers to tackle the problem of unsolicited text messages.
- As follow-up to the 'raids', my Office is currently bringing prosecutions against those companies that have sent, or allowed to be sent, unsolicited communications to subscribers or that have otherwise failed to comply with their obligations to respect the privacy of individuals. These obligations are set out in the Data Protection Acts 1988 and 2003 and in Section 13 of S.I. 535 European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2003.

My Office is fully committed to continuing its action in 2008 against those companies who flout the law in this area and who thereby infringe the privacy rights of mobile phone owners.

Where I find sufficient evidence of such offences, I will prosecute them. My Office will conduct more 'raids' as necessary in 2008. However I am hopeful that the demonstration set by the 'raids' and the prosecutions currently in train will have a significant deterrent effect on those in the sector who do not comply with their

legal obligations. In recent months we have seen evidence of such a trend in the form of a marked decrease in the number of complaints to my Office in relation to this sector. The commercial activities of the premium rate text-messaging sector are perfectly legitimate; our concern (and that of RegTel) is simply to ensure that customers are treated fairly and in accordance with the law governing the sector.

I want to acknowledge the cooperation of RegTel, ComReg and the mobile network operators and their assistance to my Office in 2007 in addressing this issue.

Sky Customer Marketing Preferences

At the end of November my Office started to receive a large number of queries from customers of Sky, the subscription TV / Communications Company. The queries related to an enclosure on data protection which they had received from Sky, amongst other items, with the December edition of the Sky magazine. These queries evolved into a proportionately large number of complaints.

Customers understood from the notice that they were required to actively opt-out from the receipt of direct marketing by mail, email, phone and text from Sky, its affiliates and unnamed third parties. Additionally, it detailed a process for the exchange of data with third parties for fraud prevention purposes. Customers seemed to be required to make contact with Sky, via a number provided in the notice, if they wished to opt-out (again) from the receipt of direct marketing material.

My Office made immediate contact with Sky and engaged intensively with it and its legal advisers in the weeks that followed. We set out to clarify the intended purpose of this notice from a data protection perspective. We pointed out the full rights granted to residents of Ireland in this area and the legal remedies available should those rights be breached. We also raised significant concerns in relation to the data sharing for credit referencing and anti-fraud purposes outlined in the notice and we sought changes in this respect. The company's view was that the notice had only sought to remind customers of how Sky handled their personal data and was not intended to alter the position in relation to their customers' previously expressed preferences. In any event, I was glad that Sky agreed to withdraw the notice in question and that the company worked with my Office on the wording of a new notice which was circulated with the February edition of the Sky magazine.

As part of the engagement I also raised certain new procedures which the company had put in place in mid-November for collecting the preferences of potential customers over the phone. I was concerned about the compatibility of these procedures with data protection law. Following additional engagement with my Office, I am pleased to say that the company amended its data collection procedures in a manner that removed any doubt about compliance with the relevant legal requirements.

Privacy Audits and Random Inspections

I am empowered to carry out privacy audits and inspections to ensure compliance with the Acts and to identify possible breaches. Such audits are supplementary to investigations carried out in response to specific complaints. They differ from the 'raids' undertaken to address unsolicited text messaging (discussed above) in that the timing of audits is usually agreed with the data controller in advance. This kind of inspection is intended to assist the data controller in ensuring that their data protection systems are effective and comprehensive. Priorities for such audits are set taking account of complaints and enquiries to the Office. During 2007 my Office continued to adopt a proactive role in this regard. In the course of the year, twelve comprehensive audits were carried out. Those audited were:

Aer Lingus
Hays Recruitment
New Ireland Assurance
Quinn Direct
Axa Insurance
Hibernian General Insurance
EBS
Carlow Credit Union
Cavan County Council
University of Limerick
The Homeless Agency
Nursing Home Repayment Scheme
Maple House Emergency Hostel

As in previous years, my inspection teams found that there is a reasonably good awareness of, and compliance with, data protection principles in the organisations that were inspected. Recommendations were made in a number of cases. I am pleased to report that the data controllers concerned were willing to put procedures in place, where suggested, to ensure that they met their data protection responsibilities in full.

In addition to the privacy audits, my Office continued with its program of random inspections following the allegations made about the mortgage brokerage and estate agent sectors on the Prime Time Investigates TV programme of December, 2006. As mentioned in my eighteenth Annual Report, my findings indicated a lack of knowledge among mortgage intermediaries in relation to the full extent of their responsibilities under the Acts. I am pleased that our ongoing liaison with the Financial Regulator and with the sector generally has produced positive results in this regard.

I would like to thank all of the organisations audited and inspected throughout the year for their cooperation. I believe such privacy audits and inspections are a very valuable tool for improving compliance with data protection principles.

Breach Notifications

During 2007, I noted an increasing trend among organisations, to date mostly in the private sector, to contact my Office directly as soon as they become

aware of accidental disclosures of customer or employee information. I welcome the trend towards voluntary disclosure as an example of good practice. It allows my Office to reassure members of the public that we are aware of the problem and that the organisation in question is taking the issue seriously. It also allows us to advise the organisation, at an early stage, how best to deal with the aftermath of a disclosure and how to ensure that there is no repetition. I hope that the development of best practice in this area is being observed by other sectors - including the public service. We were notified of eleven separate cases of accidental disclosure in the course of 2007 involving data controllers in the financial services, insurance, charity and medical services sectors. Some of these disclosures included information related to thousands of individuals or information of particular sensitivity. Of course, the practice of informing my Office and customers of a disclosure is no substitute for the proper design of systems to secure customer and employee data from accidental or deliberate disclosure to third parties.

Inappropriate Access to Personal Data

The issue of inappropriate access to information held by the public sector gave rise to increasing concern during 2007. The principal concern arose in relation to allegations that information held on all of us by the Garda Síochána (police) and by the Department of Social & Family Affairs was being routinely accessed by private investigators on behalf of insurance companies engaged in assessing claims. As part of my response I investigated the specific allegations made in relation to insurance companies. I was satisfied that there was sufficient evidence to indicate that private investigators were indeed granted inappropriate access to personal data.

To deal with this issue I prioritised the codes of practice which were already under discussion with the Gardaí and the insurance sector. The provisions of the codes place an overt focus on accountability for all access to personal data.

I also engaged extensively with the Department of Social & Family Affairs in relation to specific information which came to my attention and I found the Department to be responsive. My key concern was that the Department needed to be in a position to stand over the appropriateness of access to personal data in all cases. This requires that access to information should be restricted on a "need-to-know" basis. Furthermore, where access does take place, it must be subject to audit and follow-up if that access gives rise to any concern – in particular, improper disclosure of data. At the beginning of 2008 my Office conducted an intensive audit with the aim of assessing the situation in the Department and making recommendations for improved compliance with data protection requirements. I am hopeful that, through this process of engagement, the Department will be in a better position to meet its obligations. I will continue to liaise closely with it to this end.

DATA PROTECTION CODES OF PRACTICE

For the most part the insurance sector has engaged positively with my Office to ensure that its use of personal data is in compliance with data protection requirements. In addressing this issue, I called on the sector to take more responsibility for the actions of private investigators accessing information on their behalf. I should make clear that I raised no objection to the legitimate use of private investigators, acting within the law, to tackle suspected fraud.

In regard to information held by An Garda Síochána, it is clear that the nature of the assessment of a road traffic accident inevitably leads to contact between An Garda Síochána and insurance companies or those working on their behalf. Given the potential for temptation, I have emphasised to all concerned the importance of guarding against any attempts to seek access to additional Garda information in relation to the claimants or any relevant third party.

To further ensure compliance in this area, my Office is developing specific guidance on legitimate methods by which private investigators, instructed by insurance companies, may access personal data. This will form part of the code of practice for the insurance sector which is detailed further below. I have also liaised with the Private Security Authority with a view to ensuring that its registration requirements for investigators will include compliance with data protection obligations.

2007 marked a key year in the development of codes of practice by my Office. We worked with An Garda Síochána, the Personal Injuries Assessment Board (PIAB), and the recruitment and insurance sectors via appropriate representative bodies. All of these sectors were singled out as areas where clarification and transparency in terms of personal data and confidentiality would be beneficial.

Commissioner Noel Conroy (in one of his last public functions) and I formally launched the data protection code of practice for An Garda Síochána in November 2007. It is the first code of practice to be formally approved by a Data Protection Commissioner under the provisions of the Acts. It will not be the last.

My view is that codes of this nature benefit everybody. The Data Protection Acts provide for the preparation of sector-specific codes of practice to allow for a better understanding of the requirements of the Acts. This provision is directly transposed from a similar requirement in the Data Protection Directive 95/46/EC.

The Directive's encouragement to produce such codes is a recognition that the statutory data protection requirements can sometimes benefit from elaboration when they are applied within particular sectors. A code that is well researched, written and reflective of the processing of personal data that takes place in a sector is of enormous benefit. The provisions in our Acts allow for sectors to bring forward codes on their own behalf, for me to propose a code and even, should the circumstances warrant it, for the imposition of a code with statutory effect on a particular sector,

following approval by the Oireachtas. Equally there is provision for any code, agreed by consensus with a particular sector, to be given a statutory basis should that be deemed appropriate. However, it is perhaps understandable that sectors may initially prefer to work the provisions of a code on a non-statutory basis before seeking a statutory basis for it.

There is potential for mutual benefits for all parties from the preparation of sector-specific codes. For the particular sector involved, it applies the obligations contained in the Acts to the particular circumstances within that sector. This clarifies the standards expected and serves as a useful template for consistent training of all persons handling personal data in the sector. The sector can also benefit from the increased public and media focus on data protection standards. An increasingly discerning public can be expected to display a preference for organisations that have publicly committed themselves to high standards of data protection.

Sector-specific codes also benefit members of the public by allowing them to judge, in an informed manner, the data protection standards of particular sectors. Any concerns that they may have in relation to the security of their personal data will be addressed in the first instance by reference to the relevant provisions of the code. All parties should welcome the removal of doubts in regard to data protection standards. By facilitating all parties in understanding their obligations and rights in regard to personal data, we minimise the risk of accidental breaches of the Act and reduce the number of complaints to my Office.

Equally, a sector-specific code has practical benefits for my Office as the regulator in this area. Beyond the benefit of improving public and sectoral awareness of data protection rights and obligations, a code provides a means of simultaneously "lifting all boats" in a particular sector. Our message reaches a large number of companies in a structure fashion and compliance is correspondingly improved. It also provides a touchstone against which any complaints in relation to the handling of personal data within the sector can be assessed.

Code of Practice for An Garda Síochána

I was very pleased that the first code agreed under the provisions of the Act was with An Garda Síochána. It was a good place to start, as the Gardaí obviously hold a vast amount of very sensitive personal data. An Garda Síochána's data handling practices can have very significant implications for the relevant data subjects. The subjects of Garda information can include people who may have complained in confidence to the Gardaí, victims of crime or people under suspicion, or convicted of, committing crime. All these people have data protection rights and there is a heavy responsibility on the Gardaí to treat all personal data in their possession with respect. Fortunately the Garda authorities saw the potential of a code as a progressive tool to make data protection principles real for their employees. These obligations include only collecting the personal information they need; keeping it secure;

not revealing it to others without proper authority; and disposing of it safely when it is no longer needed.

We worked closely with An Garda Síochána to develop the code. A large number of face to face meetings were held to tease out all the issues that required clarity and to ensure that the final code would be easily understood by all parties, including members of the public. I think that we achieved our aims and the code provides a comprehensive guide to the responsibilities of Gardaí in protecting personal information. Significantly, the code also emphasises the right of each individual to get a copy of the personal data that An Garda Síochána holds about them, subject to the supply of this data not being prejudicial to investigations.

The code will not just sit on a shelf. It has been issued formally to all employees of An Garda Síochána. It provides for regular audit of access to the Garda information system. This will involve commanding officers in each Garda District examining a random selection of usage records on a regular basis to ensure that the system was used appropriately. An internal unit at Garda HQ will carry out a further audit on usage patterns. In addition, my Office will continue its regular programme of external audit of Garda data protection practices. I would like to thank An Garda Síochána for adopting such a progressive attitude towards the benefits that can flow from a code of practice on the use of personal data.

Personal Injuries Assessment Board (PIAB) Code of Practice

A code of practice agreed with the Personal Injuries Assessment Board (PIAB) was also published at the end of 2007. Previously my Office received several complaints about the level of detail revealed in claimants' medical reports. These medical reports are legitimately disclosed to relevant third parties as part of the injury assessment process. My Office recommended that the reports should only contain medical data relevant to the actual injuries being assessed. Our intervention led not just to a new code of practice, but to the alteration of PIAB application forms and medical report forms. I would like to thank all involved for their efforts in formulating and concluding a comprehensive document which serves as a guide to anyone whose personal data is being processed by the PIAB.

Now that two codes have been agreed, we are by no means resting on our laurels. For all the reasons and benefits outlined above, I am actively pursuing and finalising a code with the insurance sector as a matter of urgency. I would encourage other sectors to give consideration to such codes and to approach my Office if they wish to discuss the practical issues involved. Finally, where the nature of the processing of personal data in particular sectors gives rise to concern, I have the power to impose a code on that sector stipulating how it must process data.

PROMOTING AWARENESS

In the past year I have continued to place a particular emphasis on my awareness raising functions. Increasing awareness and understanding of data protection issues amongst the public and those entities holding personal data is mutually beneficial.

A 2005 awareness survey conducted on behalf of my Office found that 18 - 24 year olds display some of the lowest levels of awareness and knowledge of personal privacy issues and they regard such issues as having a low level of importance. In response to this finding, I decided to specifically target younger people in 2007.

At the beginning of the year, my Office engaged extensively with younger people of school going age to identify issues that impact on their privacy. We also consulted with other European Data Protection Authorities in order to evaluate key themes and messages adopted for dissemination in their countries.

In light of this, people in the 13-16 year old age bracket became a particular focus for 2007. Initially, I invited transition year pupils from the local secondary school, Coláiste Íosagáin, Portarlington, to our Office to participate in a session designed to elicit their views concerning their personal data and their right to privacy. This was followed by a series of visits and presentations to schools in the midlands area. In tandem with this programme, my Office devised a new resource book targeted at junior cycle Civic, Social and Political Education (CSPE) secondary school students.[5]

I also worked closely with the Internet Advisory Board (IAB), on which my Office is represented, and with the National Centre for Technology in Education (NCTE) in relation to online privacy issues or initiatives relevant to teenagers or their parents.

During the year, the following additional education and awareness initiatives were undertaken:

- A press release was issued to mark the inaugural Council of Europe Data Protection Day (28 January 2007),
- My Office took part in a programme for RTÉ 2FM's School Radio Project "TY Radio" (Transition Year Radio). The programme was made by students in Coláiste Íosagáin in Portarlington in association with RTÉ. A segment of the programme featured a vox-pop with students on data protection and an interview with a staff member of my Office.
- An information pack containing a themed data protection mouse mat was developed and distributed to many schools nationwide and can be requested free of charge by contacting *info@dataprotection.ie*.
- In Autumn 2007 work began on the development of a 'teenzone' web area that will be accessible from the data protection website.
- In co-operation with ComReg, my Office devised a publicity campaign to promote the new telemarketing opt-out facility of the NDD[6]. The campaign began in December 2006 with a national newspaper advertisement and was followed by a nationwide radio campaign in February 2007.
- We made 59 presentations to groups in the public, private and voluntary sectors.

5 The resource is entitled 'Sign-Up, Log In, Opt Out: Protecting your Privacy & Controlling your Data'. It is available on our website (www.dataprotection.ie)

6 The National Directory Database (NDD) is a directory enquiries tool and a basis for the production of telephone directories. It also operates as a national telemarketing opt-out register.

- My Office contributed on an ongoing basis to the broadcast and print media as data protection and privacy issues arose.

CSPE Curriculum

As referenced above, the educational resource 'Sign-Up, Log In, Opt Out: Protecting your Privacy & Controlling your Data' was written and produced by my Office in 2007. The assistance of the Curriculum Development Unit of the Department of Education & Science is gratefully acknowledged in this respect. The resource is designed for use as part of the Civic, Social and Political Education (CSPE) curriculum, which is taught and examined up to Junior Certificate level in schools. CSPE is designed to enable students to become active, aware and responsible citizens. There are 7 key concepts on the CSPE curriculum and 'Sign-Up, Log In, Opt Out' focuses specifically on two of these concepts: Rights & Responsibilities and Law. The resource can also be adapted for use in other subjects and cycles such as Junior Certificate History, SPHE (Social, Personal and Health Education), English, senior cycle Business Studies or as part of the transition year curriculum.

Within the resource itself, the development of awareness with regard to privacy and the need to protect one's personal data as a component of citizenship is linked to the fostering of other positive attitudes and values such as concern for human rights, concern for the common good and respect for the rule of the law. An awareness of how technology can affect an individual's privacy is also a core message.
I welcome wholeheartedly the inclusion of material dealing specifically with privacy and data protection in the CSPE and general curriculum. I see this development as an important validation of the relevance and importance of privacy in the everyday lives of young people. I was particularly pleased to witness the interest in the resource displayed by the Minister for Education & Science Mary Hanafin, who officially launched the resource in conjunction with my Office on the 2nd annual Council of Europe Data Protection Day on 28th January 2008.

Training Opportunities

It is, no doubt, an additional indicator of the mainstreaming of data protection that the desire on the part of organisations to avail of formal data protection training is dramatically increasing. My Office receives a large number of queries about such training. While we are not in a position to offer formal training as such, we seek to assist through presentations at appropriate events (as outlined earlier). There are also a number of training supports available through our website including a useful DVD resource. Beyond that we are actively collaborating with a number of organisations in the development of formal data protection courses and events. I view these developments as extremely worthwhile since they will further develop an understanding of data protection requirements.

A new departure in 2007 was the inclusion of data protection in conjunction with Freedom of Information

GOVERNMENT

on the course syllabus for civil servants offered by the Central Training Unit in the Department of Finance. I see this as an important development and I am currently working with the Department of Finance on fine-tuning the course. I am also examining other potential offerings in the state certification sector in addition to the existing FETAC 'Information Provider's Programme' which offers a data protection module, again in conjunction with a Freedom of Information training module.

2007 also saw the launch of a Data Protection Practitioner's Certificate by the Irish Computer Society. The course takes place over three days at the end of which attendees sit an exam in order to receive certification. I welcome this initiative and intend to monitor the development of this course.

I place a particular personal emphasis on ensuring that data protection requirements can be seen by all as part of a solution to problems rather than an extra barrier to cross. It is my strong preference that data protection issues should be addressed when proposals are at an early stage rather than have problems emerge later when change may be more difficult. In this respect, I am pleased to say that many Government departments and agencies consult my Office when developing proposals which may have data protection and privacy implications. I will continue to devote resources to the identification of privacy-friendly solutions in this context. Such consultation also complies with the EU Data Protection Directive. The Directive obliges each Member State Government to consult with its national supervisory authority when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data.

The experience of my Office is that it is usually possible, through discussion, to arrive at solutions which achieve Government objectives while minimising negative impacts on privacy. I am, of course, disappointed that some parts of the Government system seem to view my Office with caution in terms of consultation on new proposals. Too often proposals are published or new measures introduced with no attempt to seek a view from my Office. Where my Office is consulted we provide a fast and efficient response to queries received and, in the vast majority of cases, the suggestions we make are welcomed as workable and realistic. I continue to work hard to encourage all parts of Government to seek the views of my Office when bringing forward relevant proposals. In this respect, I would like to acknowledge the efforts, in particular,

of the Departments of Finance, Health and Children, Education & Science, Communications & Natural Resources and the Revenue Commissioners which have made particular efforts to seek the views of my Office on a range of issues. I have outlined below a number of examples of where my views have been sought. A large number of other public bodies have also routinely consulted with my Office and I thank them for that. I continue to seek to cooperate with the Department of Justice, Equality & Law Reform which, given its mandate, brings forward a large number of initiatives with privacy implications.

DNA Database

I was consulted by the Department of Justice, Equality and Law Reform on the scheme for the Criminal Justice (Forensic Sampling and Evidence) Bill 2007, which was subsequently published by the Department.[7] The Bill provides for the establishment of a database of DNA 'profiles' extracted from samples taken from individuals or collected from crime scenes. The purpose of the database is to assist in crime detection.

I fully acknowledge the need for the Gardaí to have access to modern means of crime detection, including DNA evidence. But it is important that the collection and retention of DNA samples and 'profiles' is proportionate and does not interfere unduly with the individual's right to data privacy.

In my comments, I highlighted my concern at the proposed indefinite retention of 'profiles' of individuals who are not subsequently convicted of a criminal offence. I suggested that the Government might consider amending the Bill to provide for the destruction of samples and profiles of persons who have not been found guilty of an offence, in line with the recommendation of the Law Reform Commission on this point[8]. I commented positively on the proposed establishment of an "Oversight Committee" to include a nominee of the Data Protection Commissioner. I suggested a specific provision that the Committee should monitor and report on the impact of the database on civil liberties.

I was very happy to note that my views were echoed in the comprehensive comments on the Bill that were subsequently submitted by the Human Rights Commission[9]. I share the view of the Commission that the Bill raises serious human rights issues which deserve to be carefully considered and debated before the Bill is finally enacted.

eBorders

In the course of the year, the Department of Justice, Equality and Law Reform sought the views of my Office in relation to the proposed eBorders system that it was seeking to progress as part of an integrated borders system with the UK. The system would collect information from all travellers as they enter and exit the State and check this data against a list of people

7 http://www.justice.ie/en/JELR/Pages/PB07000497

8 "The Establishment of a DNA Database", Law Reform Commission, Report LRC 78-2005, November 2005 at www.lawreform.ie

9 www.ihrc.ie/documents/

of concern. The basis for the inclusion of names on such a list is unclear. Additionally the initial intention is to store all information collected on a central system for a period of at least 5 years. I welcome the fact that the Department took the opportunity to consult with my Office on this matter and that several clarifications were provided to us in the course of that engagement. However the proposal, as presented to my Office, raises serious data protection issues. Among the key requirements of data protection are that information should only be collected for a specific purpose and should only be held for as long as necessary. In this current proposal, personal data in relation to all of us is to be collected each time we board a plane or a boat out of the country and this data is to be held and further used for an excessively long period of time. I await with interest the publication of firmer proposals.

Personal Public Service Number

Collection of our personal data starts in the public sector from the moment we are born. Today, everyone is assigned a Personal Public Service Number (PPSN) at birth by the Department of Social & Family Affairs (DSFA).

The PPSN was introduced in the 1998 Social Welfare Act as the unique personal identifier for transactions between individuals and Government Departments and other agencies specified in the Social Welfare Acts. Legislation regulating the use of the PPSN provides that it can be used either by the public bodies named in the Social Welfare Acts or by any person or body authorised by those public bodies to act on their behalf. While only designated public bodies can use the PPSN, equally it can only be used by such bodies for particular transactions and where the transaction relates to a public function of that body.

Our related "public service identity" - the PPSN plus our name (and any former surname), date of birth, mother's former surname, sex, nationality and address - is retained on a database in the Department of Social and Family Affairs. Recent changes to social welfare law provided for the addition of signatures and photographs. I was not consulted in relation to this and may have had some concerns in this area. This information may be shared with other agencies providing public services, subject to conditions laid down in the Social Welfare Acts.

The PPSN – originally confined to transactions with the Department of Social and Family Affairs and the Revenue Commissioners – is today increasingly demanded by public agencies as a condition for providing a wide range of services. The phenomenon of "information and function creep" is where a limited proposal is extended to purposes beyond those originally envisaged, with consequent implications for the privacy of citizens. Function creep with regard to the PPSN is a real and increasing threat. Over the last year, my Office has received numerous requests for advice on publicly-funded projects or schemes involving the gathering of the PPSN. In many cases, my Office has advised that use of the PPSN for some purposes not specified in Social Welfare legislation or for a purpose not referred to in the PPSN Register of

Users *(http://www.welfare.ie/topics/ppsn/rou.html)* maintained by the Department of Social and Family Affairs could be deemed excessive and unwarranted under the Data Protection Acts 1988 and 2003. We will continue to monitor this space closely.

Planning Issues

My Office received a significant number of complaints in recent years from people who had submitted planning applications to their local planning authorities and who felt that their data protection rights had subsequently been infringed. The complaints generally fell into three categories:

- Receipt of postal marketing from companies promoting building products, mortgages, etc.
- Publication on the planning authority website of full documentation submitted in support of planning applications, including full disclosure of all personal data contained in the documentation.
- Publication on the planning authority website of submissions or observations submitted by third parties, including full disclosure of comments of a personal nature made in such submissions.

My Office entered into discussions with the Department of the Environment, Heritage and Local Government on this matter in October 2006 to seek to establish an appropriate balance between an open and transparent planning system on the one hand and the rights of individuals to privacy and data protection on the other. The Department accepted from the outset that local authorities had clear data protection responsibilities. Accordingly, a review of the planning code was carried out to examine what changes were required to facilitate consistency with data protection requirements. Discussions concluded successfully in March 2007 with a number of significant measures to address these issues:

- The Minister for the Environment, Heritage and Local Government signed the Planning and Development (No. 2) Regulations 2007 (Statutory Instrument 135 of 2007). Amongst other things, these Regulations introduced an amended planning application form.
- The amended planning application form included, for the first time, a data protection note to inform planning applicants that the planning process is open and public and that all planning applications are made available for public inspection. It also provided planning applicants, for the first time, with an opportunity to indicate a preference with regard to the receipt of direct marketing arising from the lodging of their planning application.
- The amended form re-arranged the address/ contact details section from the front to a detachable page at the rear of the form to ensure that these personal details could be removed prior to publishing on the planning authority's website.
- The Statutory Instrument (S.I.) removed the requirement to publish the applicant's address in the weekly planning lists.

- The S.I. removed the requirement for a person making a submission or observation to submit their phone number or email address.
- The S.I. required that the weekly lists of planning applications and planning decisions should contain a banner heading with a warning to direct marketers. The warning stated that those wishing to use the personal data on the lists for direct marketing purposes should be satisfied that they may do so legitimately under the terms of the Data Protection Acts, taking account of the preference outlined by the applicants on their application form.
- In June 2007 the Department of the Environment, Heritage and Local Government published revised Development Management Guidelines for Local Authorities. These Guidelines contained significant new material concerning the requirements of the Data Protection Acts with regard to the publicising of planning applications. Where an applicant is required to demonstrate his/her links with an area or to demonstrate a need for housing, the guidelines advised planning authorities to endeavour to accept only evidence which does not contain unnecessary personal details such as an applicant's age, income, marital status, etc. The Guidelines also advised planning authorities that as long as the file in the planning office contains all documentation submitted by the applicant, there is no further requirement under the Planning Acts to publicise sensitive pieces of personal information on a website. It recommended that the planning authorities should obtain evidence that is capable of being published without breaching the privacy rights of individuals.

The implementation of these measures has greatly reduced the number of complaints which my Office receives in relation to planning matters. Ultimately, I expect that complaints of this nature will become a thing of the past as planning authorities build up an expertise in recognising the data protection aspects of their very important work.

I want to acknowledge the cooperation which my Office received from the Department of the Environment, Heritage and Local Government in bringing about significant change in this area and to commend it for addressing all of the concerns of my Office.

Health Sector

The data protection rights of individuals can take on a particular significance in relation to their sensitive health data. I know that individuals wish to be assured that their personal health data is kept confidential. I also recognise that the use of a person's data is critical to the success of their treatment and that there is also a desire to use that data to improve health outcomes for the population generally through audit and research.

Health Research Guidelines

The Data Protection Acts contain provisions to enable research to take place in the health sector on personal data under certain conditions. With this in mind, I felt that guidelines to draw these issues out might be of benefit to everyone in the field seeking to understand their responsibilities and obligations under the Acts. The need for guidelines in this area was also demonstrated by the large number of queries received from the health sector pertaining to various planned research projects.

As a first step in the formulation of the guidelines, my Office held a consultative seminar in November 2006 entitled "Promoting Health Research and Protection of Patient Rights". The seminar brought together representatives from across the health research and patient care spectrum to consider the key issues involved and to formulate an agreed approach to the development of guidelines which would take full account of data protection legislation.

The next step in the process was the circulation of a consultation document in July inviting submissions from interested parties. On foot of a number of submissions, we finalised a set of guidelines (Guidance Note on Research in the Health Sector) which is available to view in full on my Office's website. The guidelines step through the basis on which research and clinical audit in the health area can be carried out in a manner consistent with data protection legislation. They are aimed at presenting a position whereby the principles of data protection are consistent with research and clinical audit once the patient's basic right to privacy is respected.

I believe that this document provides a comprehensive overview of the data protection considerations which need to be taken into account before research involving the use of personal data can be undertaken.

I have outlined a summary of some of the main issues covered by the guidelines here:

- Anonymisation of patient records and/or freely given and informed patient consent, obtained at the first available opportunity on contact with the health system, are the foundation stones of how medical research should be undertaken from a privacy perspective. Such consent must be reinforced by information leaflets made available to patients. Where consent has not been obtained in relation to historical data and having exhausted other avenues for obtaining consent, it is possible that data controllers can examine other options (as detailed in the document) to legitimise access to such patient records.

- In relation to population registries or areas of study that require 100% coverage of the relevant population, while the Data Protection Acts allow for research carried out by the data controller, or on their behalf, without the need for express consent, this will not usually be sufficient in such cases to gather data in relation to the whole cohort of persons of interest. Equally, given the focus on the rights of individuals, the Acts do not provide a public good exemption for health research. In such circumstances and where 100% coverage is desired, specific legislation is advocated with inbuilt safeguards governing the operation of such databases.

- As with the general recommendation for research, it is recommended that the role of clinical audit teams should be described in an information leaflet provided to the patient at first point of contact with the service. The leaflet should cover the functions of clinical audit teams in reviewing the quality of care to patients generally. In situations where a direct benefit to a patient can be clearly demonstrated, or where all access to patient's personal data will take place for the purposes of audit by staff members of the health facility, it may be considered sufficient to rely upon the provisions of the Acts for processing that is necessary for 'medical purposes' and carried out by a health professional or a person "who in the circumstances owes a duty of confidentiality to the data subject that is equivalent to that which would exist if that person were a health professional".

These guidelines concentrate on the gathering of patient data for research and clinical audit purposes. Obviously the subsequent conduct of the research or clinical audit project must also comply with data protection legislation particularly in relation to access to and security of the data. This document does not seek to address these requirements but I am happy to work closely with appropriate bodies in the area to develop guidelines or codes of practice if that was seen to be helpful.

I recognise that full implementation of the approach advocated in these guidelines would result in a sea-change in the methods employed for seeking and using patient information for research purposes in the health sector. I strongly believe that the end result will be an acceptable balance in terms of the necessary availability of data for research and the protection of the individual's right to privacy.

Out of Hospital Cardiac Arrest Register

My Office also participated in a number of other engagements with the Health Sector during 2007.

The "Out of Hospital Cardiac Arrest Register" Steering Group sought the input of my Office in relation to the establishment of a register (initially in the North West region) gathering data regarding incidents of out of hospital cardiac arrests. This will be achieved through compiling different datasets held by various elements of the health sector to assist in analysing the determinants of survival/death in this area. The input of this Office to the project development phase centred around ensuring that the fundamental rights of the individual are upheld while at the same time seeking to identify approaches that would facilitate the necessary research.

Research Databases

My Office has also been involved in reviewing a number of ambitious research projects to ensure that the obligations set out in the Data Protection Acts are fully reflected in the operation of the projects. There was extensive engagement in relation to the development by a consortium of a research biobank for the study of prostate cancer. I hope that the template agreed for this project can be replicated when other groups approach my Office for advice.

Similarly, discussions are ongoing with the Irish Cervical Cancer Screening Research Consortium which requested our views in relation to the setting up of a research database.

Work with the HSE (Health Service Executive)

My Office also participated in the HSE's Information Sharing Framework Working Group meetings which were convened to agree Information Sharing Guidelines for use by Primary Care Teams. Again, in this case, the role of the Office was to ensure the compliance of the guidance material with the principles set out in the Data Protection Acts. We also participated in a HSE initiative to discuss the Research Ethics Committee structure. I welcome the work being done by the HSE nationally in this area and my Office will offer ongoing assistance in this matter.

This is in addition to providing advice to constituent elements of the HSE on an ongoing basis in relation to specific queries received.

NHO Code of Practice

As indicated in last year's report, my Office provided input to the drawing up by the National Hospitals Office of a Code of Practice for the management of records in the health sector. A very impressive Code was launched in May of last year and my Office continues to provide support for the roll-out of the code which has been made available to each employee in the health sector. The code outlines in all key areas the measures to be undertaken to ensure consistency of health records and compliance with the requirements of the Data Protection Acts. The code is a model of the type of guidance which can be given by organisations to all employees to ensure compliance with its legal obligations in relation to data protection.

National Cancer Registry of Ireland – Guidelines regarding data confidentiality in the Registry

My Office was consulted in relation to a revised set of guidelines on the release of confidential data in the National Cancer Registry. The Registry was established by the Minister for Health in 1991 and its functions

include the collection, classification, analysis and storage of information relating to the incidence and prevalence of cancer in Ireland. It also promotes and facilitates the use of the data in approved research and in the planning and management of services. Given the special provisions which exist for the provision of information to the registry as contained in the Health (Provision of Information) Act 1997, I understand the Registry's interest in having a set of guidelines ('Data confidentiality in the National Cancer Registry') in place to demonstrate exemplary standards of confidentiality. The document was published in April 2007 *(www.ncri.ie)* and should serve as a model for other organisations controlling sensitive personal data in the health area. In particular, an absolute requirement for the consent of patients before individual data can be released is set out as a minimum standard.

Medical Council Guidelines

My Office was invited to submit comments to the Medical Council in the course if its preparation of the 6th Edition of its "Guide to Ethical Conduct and Behaviour". These ethical Guidelines complement data protection principles and do so in a concise manner.

TECHNOLOGY DEVELOPMENTS

Web 2.0

New and existing technology, particularly the changing patterns of web usage, is a continuing challenge facing my Office. While the related privacy issues have not yet found expression as a proportionately large number of complaints to the Office, I have devoted attention to these issues in an attempt to ensure that privacy is built into such technologies from an early stage (and thus avoiding complaints in the future).

Web 2.0 is the term that has been settled upon to describe the next phase of development of the web. This phase of development is providing new ways for people to interact with each other and to exchange information. We are seeing a surge in the use of social networking sites and the web has become dominant as a means of communicating.

To deal with the issues to which this gives rise, my Office has sought to engage with some of the leading companies in the sector, such as Google, Facebook and Bebo. I will continue to do so; the investment of time and resources will be fully justified if we can ensure that the privacy expectations of users are respected. So far I am encouraged as I perceive that these companies are taking their responsibilities seriously.

Search Engines

A significant amount of privacy-related media coverage in the technology field in 2007 was devoted to the appropriate period for the retention of search logs and IP addresses by search engines (much of the attention was focused on Google). The retention of our personal information, by both the State and commercial entities, is becoming an increasingly important issue. The cost of storage of information has reduced until it is now almost economically more advantageous to retain information than to delete it. However, a key principle of data protection is that personal data should only be retained as long as the reason for which it was given remains valid. This imposes a requirement on all entities holding such information to put in place policies to ensure that personal data is deleted once the business need for holding it has expired. This is even more important when one considers the type of personal information that would be revealed through a detailed history of our personal use of search engines.

Thankfully, and prompted largely by the attention focused on the issue by the Article 29 Working Party of EU Data Protection Authorities, a certain competition developed between search engines in relation to the minimum period for holding such information. This was most welcome and is a testimony to the growing relevance of privacy to the companies' bottom line. As I mentioned in last year's report, those entities that are seen to take privacy seriously are increasingly attracting consumers; those entities that are exposed as less concerned about privacy are suffering.

Helpfully, as the debate on this issue proceeded, the focus expanded beyond a narrow Google-only concern to incorporate the other players in this area (albeit that Google commands a large segment of the market at this point). The Article 29 Working Party is expected to issue an Opinion on the issue in the course of 2008.

Social Networking

There is little doubt that the huge growth in the use of social networking sites is set to continue. This is an issue which I touched upon in my report last year. My experience in the interim has confirmed my view that companies in this area appear to be taking their privacy responsibilities seriously.

In general, these sites do care about privacy issues and have sought to better understand their obligations from a data protection perspective. Equally, as one service provider put it, such sites are commercial ventures and not public utilities. However, I expect that extensive information should be available to users so that they can make informed service choices in relation to the privacy options available on these sites. Additional difficulties arise in relation to the posting of personal information by third parties, such as a picture of a teacher in a classroom posted without their consent. In these cases an active and up-front complaints handling system in relation to privacy issues is required, with penalties for users misusing the service.

Biometrics

My Office continues to receive an ever-increasing number of queries and complaints from the public about the deployment of biometrics for a range of purposes. Biometric data is created from various physical or physiological characteristics of a person. Most commonly, biometric systems are based on recognition of an individual's fingerprint but biometric technology can recognise an iris, a retina, a face, DNA etc. Different biometric systems may store raw or encrypted data that can be used to generate an image, or they may store encrypted partial data that cannot be used to generate an image but is sufficient to recognise the relevant individual. Until recently, most of the concerns raised with my Office concerned the use of biometric systems for the recording of time and attendance in the workplace. A substantial guidance note was published on our website as an aid to employers seeking to use such a system and to make them aware of their responsibilities under the Data Protection Acts. The guidance note made it clear that all situations must be judged on a case-by-case basis and that it is the use of a biometric system by an employer that may be of concern from a data protection perspective.

During 2007 new concerns about the use of biometrics in Ireland were brought to my attention. Most disturbingly, the introduction of biometrics by places of education, including some secondary schools, for the recording of attendance emerged as an issue of great concern. In addition, I received complaints about the introduction of biometrics for access purposes from members of some leisure centres.

The widening use of biometric data and the effect that the processing of such data may have on daily life concerns me greatly. There is undoubtedly a risk that the general public will become desensitised by the roll-out of biometrics. The introduction of such systems in the school environment will, without question, serve to make children less aware of their privacy and data protection rights. Accordingly, I published guidance for schools, colleges and other educational institutions on this specific subject as soon as the matter came to my attention (the relevant guidance note is re-produced in full in the Guidance Section of this Annual Report).

This guidance note draws attention to the need to consider the proportionality of introducing a biometric system from a data protection perspective. It also emphasises the requirement to obtain the signed consent of the student users (and the consent of parents or guardians in the case of minors) giving them a clear and unambiguous right to opt out of the system without penalty. I expect all educational institutions to consider fully the issues which I have addressed in detail in the guidance note before they embark on the deployment of a biometric system. Furthermore, my guidance on the obtaining of consent is clear and explicit. I will have no hesitation in using my full powers against any educational institutions that ignore this guidance and breach the data protection rights of their students.

With regard to the utilisation of biometrics in the workplace to record time and attendance, I will continue to examine each situation which comes to my attention on a case-by-case basis taking account of the published guidance in this area. In particular, I

will be examining the justification put forward by each employer for the introduction of biometrics in order to ensure that it complies with the data protection principle of proportionality. Apart from a case on which I reported in my Annual Report for 2005, no other workplace, in the many cases which I have examined, has been able to demonstrate that the deployment of a biometric system allowed it to over-ride the right of individual workers to object to its use. The obligation to respect such an objection involves provision of an alternative, non-biometric system for those employees who object. An example of a workplace using biometrics which was investigated by my Office (following receipt of complaints from some of its employees) is set out in the case studies.

INTERNATIONAL RESPONSIBILITIES

Article 29 Working Party

During the year, the Office maintained its active involvement with the Article 29 Working Party. We participated in each of the Working Party's plenary meetings as well as in a number of its sub-groups.

The Working Party is provided for in Article 29 of the EU Data Protection Directive 95/46/EC. It acts as the principal co-ordination mechanism among EU data protection authorities. Its work helps to promote a more uniform application of the provisions of the Directive throughout the European Economic Area. It also acts as an adviser and advocate when data protection issues arise at European level.

Definition of "Personal Data"

In its Opinion 4/2007, the Working Party examined exhaustively the core issue of what constitutes "personal data" within the meaning of the Data Protection Directive. Taking the 4 key elements of the definition – "Any information …..Relating To ….an Identified or Identifiable …..Natural Person" - the Opinion describes both the wide scope of the definition and how it should be interpreted in practice, using illustrations. The Opinion is of considerable value to data controllers and to specialists in the area of data protection.

International Data Transfers - Binding Corporate Rules

The EU Data Protection Directive and the Data Protection Acts impose conditions on the transfer of personal data to countries outside of Europe that are not considered to provide an "adequate" level of data protection. In broad terms, a data controller that has a need to transfer large quantities of personal data outside of Europe must put in place a contract that ensures that the transferred data will benefit from European standards of data protection. The EU Commission has approved a number of 'model contracts' that can be used for this purpose.

In order to facilitate multinational companies with operations in many countries, the Working Party has developed an alternative system of "Binding Corporate Rules" (BCRs). BCRs allow the composite legal entities of a corporation (or conglomerate) to jointly sign up to common standards for the processing of personal data which are compatible with EU data protection law. This avoids the need for individual contracts between EU and non-EU subsidiaries for the transfer of personal data between them. In order to facilitate corporations wishing to apply for approval, the Working Party, in its Recommendation 1/2007, approved a standard application form, based on a model put forward by the International Chamber of Commerce.

I hope to see further progress in the use of BCRs to ease the process for the transfer of personal data for business. In this respect, I recognise that a consistency of approach between Data Protection Authorities would be immensely beneficial and I will certainly work towards that goal.

International Data Transfers - Passenger Data (PNR)

In the course of the year, a revised Passenger Name Record (PNR) agreement was negotiated with the United States by the EU. The agreement provides for the transfer of passenger data from airline reservation systems to the US immigration authorities, subject to certain safeguards. In its Opinion 2/2007, the Working Party sets out the information on the PNR arrangement that should be provided to affected passengers.

SWIFT

Another issue which first arose in 2006 and continued into 2007 was a concern at the ongoing access by the US authorities to records held in a mirror site in the US for the SWIFT inter-bank funds transfer system. This site contains details of all inter-bank transfers throughout the world and is not just limited to those originating or terminating in the US. The legal basis for the transfer of the personal data collected in the EU to the US was resolved by certain actions by SWIFT, including signing up to the EU-US Safe Harbour agreement which is an EU-recognised system for legally transferring personal data to the US from the EU for certain qualifying

entities. Additionally, the EU and the US entered into an international agreement which included undertakings from the US as to the use that would be made of any personal data accessed from the system.

In terms of how this issue was progressed in this country, I am very grateful for the excellent co-operation which my Office received from the Irish Bankers Federation which greatly assisted in ensuring that Irish financial institutions were among the first to comply with the legal requirement to provide notice to customers of the transfer of their data to the US and potential access by the US authorities.

Electronic Health Records (EHRs)

As described in last year's Annual Report, the Working Party finalised a working document (WP 131) on electronic health records on which comments were invited. The focus of the document is on the provisions of Article 8 of the Data Protection Directive and their relevance as a basis for the processing of personal information in EHRs. The document provides a useful reference point for any such system developed in this country or in other Member States.

Domestically, I have identified engagement on any discussions around the introduction of a national EHR system as a priority in order to ensure that full account is taken of privacy concerns at an early stage of development.

Working Methods

In the course of the year, the Working Party reviewed its working methods. It decided to publicise its work more widely; this included making its agenda and minutes publicly available on its website. The agreed actions are described in its document WP 135. It also embarked on a review of its effectiveness, based on an examination of the impact of its Opinions on data protection practice.

Other Activities

The Working Party also issued Opinions on:

- the Commission Green Paper on Detection Technologies (Opinion 1/2007);
- the proposed Regulation on Visas (Opinion 3/2007);
- the Consumer Protection Cooperation System (Opinion 6/2007);
- the Internal Market Information System (Opinion 7/2007);
- the level of protection of personal data in Jersey (Opinion 8/2007);
- the level of protection of personal data in the Faroe Islands (Opinion 9/2007);
- the 8th Directive on Statutory Audits (Opinion 10/2007);
- the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes.

The Working Party also issued a Report evaluating the joint enforcement exercise carried out in the health insurance sector (Report 1/2007).

All of the Working Party's documents are available on its website *(http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2007_en.htm).*

Third Pillar Groups

The formal advisory role of the Article 29 Working Party is limited to the First Community Pillar of the EU. The Office is also represented at meetings in Brussels of groups dealing with Third Pillar issues (police and judicial cooperation in criminal matters).

- *EUROPOL Joint Supervisory Body (JSB)*
  The EUROPOL JSB is an independent body that draws its membership from all EU national data protection authorities including my Office. EUROPOL (the European Police Office) enables European police authorities to share information about certain kinds of serious crime. The EUROPOL JSB reviews the day-to-day activities and plans of EUROPOL to make sure that the organisation's storing, processing and use of personal data does not violate the rights of the individual. The Office of the Data Protection Commissioner is also the national supervisory body with responsibility for monitoring the liaison between An Garda Síochána and EUROPOL to verify that data protection safeguards are respected.
- *Customs Information System Joint Supervisory Authority (JSA)*
  The Customs Information System JSA is another independent body that draws its membership from EU national data protection authorities. It supervises the European Customs Information System based in Brussels to ensure that personal data within the system is processed in a manner that respects the data protection rights of individuals.
- *Schengen Joint Supervisory Authority (JSA)*
  A Schengen Information System exists to process information relevant to the free movement of people across borders within the Schengen area. As Ireland is not a full member of Schengen, we attend meetings of the Schengen JSA in an observer capacity.
- *EURODAC*
  EURODAC is the EU central database for the recording and comparison of the fingerprints of asylum seekers. While the European Data Protection Supervisor (EDPS) has overall responsibility for the data protection supervision of the EURODAC Central Unit, the Office of the Data Protection Commissioner participates in regular EURODAC supervision coordination meetings between European data protection authorities and the EDPS. We also have responsibility for overseeing the operation of the EURODAC system in Ireland from a data protection perspective.
- *EUROJUST Joint Supervisory Body*
  EUROJUST facilitates the investigation of crimes with a cross-border dimension by aiding cooperation between judicial and prosecution

authorities. The Office of the Data Protection Commissioner is represented on the EUROJUST JSB, a supervisory body that ensures that personal information is processed by EUROJUST in a manner that respects the data protection rights of individuals.

Key areas of concern in these meetings during 2007 included:

- The adoption of a common position regarding the use of the concept of "availability" in law enforcement. "Availability" is the term used to describe a new agreed concept in law enforcement cooperation in police and judicial cooperation at EU level. It means that, in principle, information held by law enforcement agencies in one EU jurisdiction will be made available to law enforcement authorities in other EU jurisdictions on request. EU data protection authorities, including the Irish Data Protection Commissioner, are concerned that the data protection regime that currently applies to law enforcement cooperation is not strong enough to protect the data protection rights of people living and working in the EU from abuse through the application of the principle of "availability".
- They are also concerned that the replacement regime that was being finalised towards the end of 2007 does not contain sufficiently robust data protection standards. the development of a common opinion regarding the question of a new legal basis for EUROPOL. Work is already underway to change the legal basis under which EUROPOL operates to make it more efficient and adaptable. The EU's data protection authorities are working to ensure that the new legal text takes adequate account of individual data protection rights.
- The enforcement of the right to know and to exercise control over how EU law enforcement cooperation agencies are using your personal data. In this context the data protection authorities work together to ensure that the various agencies active in law enforcement and judicial cooperation respect individual access rights. The data protection authorities also inspect the databases used by law enforcement cooperation agencies to ensure that personal data is being processed in a manner compatible with applicable data protection standards.

OECD Engagement

As I have said on a number of occasions, measures to protect the data of individuals cannot be solely focused on our own borders given the increasing globalisation of business. To be able to regulate effectively the use of personal data on a global basis, effective co-operation mechanisms with other data protection and privacy enforcement authorities are necessary. In the EU, the Article 29 Working Party provides the main conduit for such co-operation. However, privacy abuses are clearly not confined only to EU and EEA member states and in that context my Office has sought to contribute to the work of the OECD in improving the mechanisms for co-operation between data protection authorities across the globe. The OECD Council in June approved a Recommendation on the modalities of such co-operation (www.oecd.org/dataoecd/43/28/38770483.pdf). I fully support this work and my Office will be contributing further as we approach the implementation phase.

Safe Harbour[10] Conference, Washington

I am also increasingly concerned to ensure that the best information is provided to companies in relation to the options available for the transfer of data out of the EU. In this respect my office attended and spoke at the Safe Harbour Conference in Washington in October.

Other International Meetings

The Spring Conference of European Data Protection Authorities, hosted by the Cypriot Data Protection Commissioner, discussed such issues as media and personal privacy and children's personal data. It led to the formal establishment of the Working Party on Police and Justice. This European-level group of data protection authorities has a mandate to monitor and examine developments in the area of police and law enforcement generally. In this context it seeks to meet the growing challenge of protecting individual rights with regard to the processing of personal data. The Working Party has provided a useful forum for discussion of issues such as the new European Council Decision on the stepping-up of cross-border cooperation, particularly in combating terrorism and cross-border crime, and the Framework Decision on Data Protection in the area Of EU cooperation on justice and home affairs matters.

10 Safe Harbour is a system of certification of US companies as privacy friendly destinations for transfer of personal data from the EU.

I also participated in the 29th International Conference of Data Protection and Privacy Commissioners, hosted on this occasion by the Canadian Privacy Commissioner. The Conference focused on new challenges facing Data Protection and Privacy Commissioners, varying from new communications technology to the increasing demands of public security and law enforcement with regard to personal data. I am pleased that my Office was able to contribute to the conference by collecting and analysing the expectations of the various participants at this and previous conferences, with a view to making the conference as effective as possible in the future.

We also continued to maintain close informal contacts with other data protection authorities, particularly with the Information Commissioner's Office in the United Kingdom. I contributed to a conference on data sharing in the public sector which was organised in Belfast by the Assistant Commissioner for Northern Ireland. I also participated in the annual BIDPA meeting, hosted on this occasion by our colleagues from Guernsey. The close cooperation between data protection authorities throughout the islands and beyond was given special recognition early in 2008 when President McAleese hosted a reception for them in Áras an Uachtaráin

ADMINISTRATION

New Registration Regulations

Under Section 16 of the Data Protection Acts, my Office maintains a public register of particular categories of entities in both the public and private sectors that process personal information. Members of the public can consult this register on our website to discover how a particular company uses their information, what type of information is held and who is given access to the information. From 1st October 2007 new regulations (S.I. No. 657 of 2007) came into effect determining the categories of data controllers and data processors who must register. The obligation to register was dropped for a number of categories, notably solicitors and barristers, educational institutions and public representatives. Subsequently my Office engaged in an ongoing process of informing data controllers and data processors about the new requirements, to ensure that those required to register comply with the regulations and to ensure that the information on the register is relevant, accessible and accurate.

In 2007 the number of organisations registered with my Office decreased by 681 or 10.7% (see appendix 2), reflecting the impact of the new regulations.

Our on-line registration system continues to provide data controllers and data processors with a customer-friendly, efficient means of submitting their registrations and we are continuing to develop the system further over time to maximise the efficiencies it can offer both to customers and to the Office.

Processing of Genetic Data for Employment Purposes

From 8th October 2007 the new Data Protection (Processing of Genetic Data) Regulations (S.I. No. 687 of 2007) came into operation. The effect of these regulations is to designate the processing of genetic data in relation to the employment of a person as processing that can only take place with the prior approval of the Data Protection Commissioner. The regulations are a response to the danger that predictive genetic testing might otherwise provide a basis for discriminatory treatment in regard to employment. We have thus far not received any applications for prior approval in this area.

Running Costs

The costs of running the Office in 2007 were as follows:

	2006 (€)	2007 (€)	% change
Overall Running Costs	1,281,521	1,835,155	43.20% increase
Receipts	586,817	535,405	8 .76% decrease

A fuller account of income and expenditure in 2007 is provided in Appendix 3.

PROCESSING DATA

The wheel diagram below will help you understand the many ways in which personal data may be processed.

- Your personal data must be processed in accordance with the Data Protection Acts, 1988 and 2003.

  Processing the data covers a whole range of activities with regard to personal data. The Data Protection Acts apply to all personal data held manually in a filing system or electronically.

PART 2 - CASE STUDIES

Case Study 1: Right of Rectification of Personal Data Held by a Data Controller

I received a complaint regarding a medical report carried out at the request of the complainant's employers. The report was a psychological assessment dealing with the complainant's ability to return to her original workplace after a period of absence on sick leave.

The person concerned had received a copy of the medical report in question from the medical practitioner who carried out the assessment and she considered the contents to be inaccurate. The complainant then requested that the report be rectified to reflect what she considered to be an accurate description of her particular circumstances. However, the data controller, a consultant psychiatrist, reverted to the data subject stating that it was not possible to make the kind of alterations to the independent medical assessment that had been sought.

Under Section 6 of the Data Protection Acts 1998 and 2003, if you discover that information kept about you by a data controller is factually inaccurate or collected unfairly, you have a right to have that information rectified or, in some cases, you may have that information erased. However, this is not an unqualified right and depends on the circumstances of each case. The judgement to be made in such cases is complicated all the more when the matters at issue are medical in nature. If for example, a data controller - in this case, the medical practitioner - considers that data is, in fact, accurate and if the data subject disagrees, then one possible course in the interest of achieving an amicable resolution is for the data controller to annotate the data to the effect that the data subject believes that the data is inaccurate for reasons which should be indicated (this solution is explicitly provided for in Section 6(1)(a) of the Acts).

This course of action was followed in this case and as part of the rectification process, the complainant supplied various annotations to be included in the medical report. Also supplied with each of these annotations was a detailed explanation for such. Having examined the annotations and all the information my Office had to hand, including the medical report in question, my Office was of the opinion that the proposed annotations supplemented the medical report without changing the report materially.

My Office communicated its position to both parties and the medical practitioner concerned helpfully supplemented the medical report in question by inserting the requested annotations. This allowed for the complaint to be resolved to the satisfaction of all parties concerned.

This case clearly indicates the value of the right of an individual to seek the rectification or supplementing of personal information relating to them, in accordance with Section 6 of the Data Protection Acts, 1998 and 2003. In instances such as the case highlighted above, where the personal information is of a subjective nature, the right to rectification is not always appropriate. In this case the individual concerned was satisfied that the annotations she supplied, when recorded with the report, were sufficient to ensure that anyone reading the report had a balanced view of her circumstances.

Case study 2: Data Controller breaches several provisions in its processing of Sensitive Personal Data

I received a complaint in May 2006 from a data subject regarding the use by her former employer, Baxter Healthcare S.A., of two medical reports relating to her. The data subject had been involved in an industrial accident at work in April 2002 which subsequently resulted in a prolonged absence from the workplace. During this absence, the data subject pursued a personal injuries claim against Baxter Healthcare. As part of this process, at the request of the solicitor acting on behalf of Baxter Healthcare's insurers, she attended a consultant neurologist on two occasions for medical evaluation in 2003 and 2004. Early in 2005, the data subject became aware that the medical reports compiled as a result of those evaluations were in the possession of Baxter Healthcare. Through her solicitor, the data subject made an access request to Baxter Healthcare for copies of the medical reports. She was advised in writing that, as these reports were obtained in the context of her personal injury proceedings, her access request should be addressed to the solicitors, P. O'Connor & Son, acting for the insurers. Shortly afterwards, the data subject's contract of employment was terminated. The decision by Baxter Healthcare to terminate the employment was stated to be on the basis of the medical evidence available to the company, including the medical reports compiled in 2003 and 2004 in the context of the data subject's personal injury claim. Following her dismissal, the data subject brought a claim to the Labour Relations Commission against Baxter Healthcare under the Unfair Dismissals Act 1977 to 2001. A hearing in relation to this case took place in April 2006 and the data subject alleged that, in the course of the hearing, copies of the medical reports were furnished by Baxter Healthcare to herself, to the Rights Commissioner and to all present. These medical reports had not been previously provided to her in response to her access request.

My Office conducted a detailed and extensive investigation of this complaint. This focused on 2 primary data protection issues, namely the use of the medical reports obtained to defend an insurance claim to support the dismissal of the data subject and the disclosure of those same medical reports at a labour relations hearing. The company's solicitor stated that the medical reports of the consultant neurologist were obtained for the legitimate purpose of defending personal injury proceedings instituted by the data subject and that the medical reports were also employed and required for the legitimate purpose of defending separate legal proceedings against Baxter Healthcare under the Unfair Dismissals Acts 1977 to 2001. It submitted that Section 2(1)(c)(i) of the Acts specifically envisages that the data may be obtained and used for more than one purpose, provided that both purposes are legitimate. It went on to state that Section 2(1)(c)(ii) of the Acts only prohibits further processing insofar as that processing is incompatible with the original purpose or purposes. It argued that the use of the reports to defend legal proceedings against Baxter Healthcare under the Unfair Dismissals Act could not be said to be incompatible with the original purpose as the original purpose was to defend legal proceedings instituted by the data subject and the subsequent use was to also defend legal proceedings, albeit separate proceedings by the data subject.

The data subject sought a decision on her complaint under Section 10(1)(b(ii) of the Acts in June 2007. In my analysis of the data protection issues arising from this complaint, I found that the medical reports in question constitute 'sensitive personal data' within the meaning of the Acts. The medical reports were commissioned on behalf of Baxter Healthcare's insurers, by its solicitors, for the purpose of the defence of the High Court personal injury claim instituted by the data subject. The reports were, however, used for three purposes:

- They were used for the purpose for which they were generated in the first place, i.e. for the defence by Baxter Healthcare's insurers of the High Court personal injury claim instituted by the data subject.
- They were used in the decision taken by Baxter Healthcare to terminate the employment of the data subject.
- They were used to defend legal proceedings taken by the data subject against Baxter Healthcare under the Unfair Dismissals Act at a hearing in April 2006.

No data protection issue arose in relation to the first use of the medical reports by Baxter Healthcare's insurers in the context of its defence of the personal injury claim brought by the data subject.

With regard to the second use by Baxter Healthcare of the medical reports in the decision to terminate the data subject's employment, this was done without the data subject's consent. The general requirements that must be complied with by a data controller under the Acts in relation to the personal data of a data subject include the following:

- the data shall have been obtained only for one or more specified, explicit and legitimate purposes
- the data shall not be further processed in a manner incompatible with that purpose or those purposes
- the data subject is informed of the purposes or purposes for which the data are intended to be processed

The consent of the data subject is the default position, as it were, for the fair processing and obtaining of personal data. Where it is absent, the data controller may not process personal data unless it can find another basis in the Acts. The Acts provide for the following exemptions which were potentially applicable in the present case:

- the processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the fundamental rights and freedoms or legitimate interests of the data subject (Section 2A (1)(d));

and (because sensitive data is involved)

- the processing is required for the purpose of obtaining legal advice or for the purposes of, or in connection with, legal proceedings or prospective legal proceedings or is otherwise necessary for the purpose of establishing, exercising or defending legal rights (Section 2B (b)(vii)).

All of these conditions must be met.

In my analysis of this complaint, I considered that the purpose for which the medical reports were originally obtained (the defence by Baxter's insurers of the High Court personal injury claim instituted by the data subject) was not compatible with their further use to support the data controller's decision to dismiss the data subject. I considered that, in the absence of the data subject's consent, this processing of the data subject's sensitive personal data constituted a breach of the Acts.

With regard to the third use by Baxter Healthcare of the medical reports to defend legal proceedings under the Unfair Dismissals Act, the same considerations arose in relation to the further use of the sensitive personal data at a hearing before a Rights Commissioner in April 2006, with the aggravating factor that the sensitive personal data was further disclosed to those involved in the hearing.

However, I had to consider if the processing of personal data in this case might benefit from the exemption in Section 8(f) of the Acts which provides that: "Any restrictions in this Act on the processing of personal data do not apply if the processing is ...required...for the purposes of, or in the course of, legal proceedings in which the person making the disclosure is a party or a witness."

I formed the opinion that this exemption cannot apply to sensitive personal data which has already been improperly processed to support the decision (dismissal) which was the subject matter of the legal process. I concluded that the use of the medical records to defend the Unfair Dismissals claim constituted a further breach of the Acts.

For completeness, my Decision in this case also found that Baxter had failed to comply fully with an access request made by the data subject.

This case demonstrates the care which data controllers must exercise in the processing of all personal data, including sensitive personal data, in its possession. It is unacceptable for a data controller to seek to take advantage of personal data which may be in its possession and to use it for some purpose unrelated to the purpose for which it was originally obtained.

Case Study 3: Inappropriate use of CCTV footage by West Wood Club

I received a complaint from a data subject alleging breaches of the Data Protection Acts by inappropriate use of CCTV footage at West Wood Club, Sandymount in Dublin. In her complaint she informed my Office that on 4th March, 2006 she visited the West Wood Club as a member to use the steam/sauna rooms and the swimming pool. A customer service issue arose in relation to the cleanliness of the facilities on the day which were the subject of a phone-call by the complainant from the steam/sauna rooms. The data subject wrote a subsequent letter of complaint about the matter to the Club following which she was asked to meet the manager to discuss the matter. Upon doing so she was presented with CCTV footage which it was claimed supported the club's view of the customer service issues arising and refuting the claim that she had made a phone-call on the issue on the morning in question. In this respect, three CDs of CCTV footage were presented each of which in turn were claimed to be the data subject engaging in leisure activities within the gym on the morning in question. They in fact were not the data subject and were other female members of the gym.

Shortly afterwards the data subject's membership of the gym was revoked.

The data subject informed my Office that she found it acceptable to be shown CCTV footage to assure her that the sauna/steam rooms had been cleaned but she found it unbelievable that West Wood Club kept and viewed footage to discredit members' genuine complaints. She felt strongly that the CCTV footage was shown to her to intimidate her and question her good character and was used to say that she was lying.

My Office commenced an investigation and wrote to the Managing Director of West Wood Club expressing our concern at what appeared to be excessive and disproportionate use by West Wood Club of CCTV footage for the purpose of dealing with the data subject's complaint. A response was received from the solicitors for the Club and an exchange of correspondence subsequently took place between my Office and the solicitors. Among other things, my Office was informed that the only purpose for which CCTV was used in the Club was for security. They also confirmed that members and staff of the Club were aware that their images were being recorded as there were several signs displayed in the Club regarding the operation of CCTV. It was also confirmed to my Office that CCTV footage was automatically erased at the end of each month.

However, the Solicitors contested any suggestions that the Data Protection Acts prohibit data that has been bona fide obtained and temporarily stored for one general purpose from being used in specific circumstances for some other useful purpose that is for the general good. They also stated that the purpose of the CCTV system in operation at West Wood Club was, like most CCTV systems, security and that this included the issues of theft and personal safety and integrity. They contended that this was a health and safety issue, coming under the general heading of

security, on the grounds that the data subject made a complaint that the sauna was unhygienic because it had not been cleaned. I disagreed with the data controller's position on this matter. I accepted that the purpose of 'security' may include the issues of theft and personal safety in certain circumstances related to security risk. However, the issues of integrity, health and safety are clearly separate purposes to the purpose of 'security.'

Section 2(1)(c)(ii) provides that data shall not be further processed in a manner incompatible with that purpose or those purposes for which it was obtained. It was clear from my Office's correspondences with the data controller's solicitors that West Wood Club processed images which were recorded for 'security' purposes by showing them to the data subject in response to a complaint which she had made concerning the sauna/steam rooms not being operational on the morning of 4 March, 2006. Her complaint had nothing whatsoever to do with 'security' issues and, therefore, it was entirely inappropriate for the data controller to produce personal data, about other individuals as it transpired, which was obtained for 'security' purposes, to attempt to deal with this matter.

I had no reason to doubt the version of events given to me by the data subject. I concluded that West Wood Club did indeed set out to refute the data subject's complaint through the use of CCTV footage which was recorded for a 'security' purpose.

I was required to make a Decision on this case under Section 10(1)(b)(ii) of the Acts. I formed the opinion that West Wood Club breached Section 2(1)(c)(ii) of the Acts by the further processing of CCTV footage which was obtained for security purposes in a manner incompatible with that purpose. I found it disturbing that the data subject's membership of West Wood Club was invalidated following a breach of the Data Protection Acts by West Wood Club. It is unacceptable that an entity against whom a complaint is made would contravene the Data Protection Acts in dealing with the complaint and thereby infringe on the data protection rights of the complainant or others.

CCTV recordings have become an everyday part of our lives. Their usage, and seeming acceptance, for so many different purposes is troubling. In this case, the use of CCTV in the private areas of a sauna/steam room in a gym is questionable in itself from a data protection perspective. To then use the footage captured (notionally for security purposes) in an attempt to discredit a gym member making a customer service complaint is totally unacceptable. In the circumstances I had no hesitation in finding in favour of the complainant.

Case Study 4: NewTel Communications - Ordered to suspend marketing

The marketing activities of the telecommunications company NewTel Communications Ltd came to the attention of my Office in 2006 and again early in 2007. In 2006 an inspection was conducted of its marketing activities and appeared to indicate that it had taken appropriate remedial activity. However, in 2007 we received in a short period a number of complaints regarding marketing calls made by this company. These calls were made to individuals who either had already expressly told the company that they did not wish to be contacted or had exercised their right to have their preference not to be called recorded on the National Directory Database opt-out register.[11]

These marketing calls contravened Regulations 13 4(a) and 13 4(b) of SI 535 of 2003 which state that:

"A person shall not use, or cause to be used, any publicly available electronic communications service to make an unsolicited telephone call for the purpose of direct marketing to the line of a subscriber, where -

(a) the subscriber has notified the person that the subscriber does not consent to the receipt of such a call on his, her or its line, or

(b) subject to paragraph (5), the relevant information referred to in Regulation 14(3) is recorded in respect of the line in the National Directory Database."

My Office investigated the complaints which we had received. After initial investigation, we found out that an external offshore agency employed by NewTel Communications Ltd to make marketing calls was not following the company's "do not call" policy. As a result of this information, NewTel Communications Ltd ceased its relationship with the offshore agency concerned in March 2007. However, my Office continued to receive complaints about further unsolicited calls made by NewTel Communications Ltd. We concluded that, despite assurances from the company, its marketing procedures were not sufficiently robust or watertight to uphold the data protection rights of subscribers who did not wish to receive direct marketing calls. We accordingly requested NewTel Communications to cease all 'cold call' marketing with immediate effect or we would issue a legally binding enforcement notice to that effect. We informed the company that we would not agree to allow this marketing activity to recommence until it had identified and remedied whatever problems in its procedures or systems had led to the unsolicited marketing calls to the complainants to my Office.

NewTel Communications Ltd complied with my Office's request and it initiated an internal investigation. As a result of this investigation, the company established that a second offshore agency was not following the company's "do not call" policy. Recognising the seriousness of the matter, the company suspended this agency from marketing on its behalf. My Office was satisfied with the actions taken by the company to identify the problems and to correct them. Following this remedial action, we agreed that NewTel could recommence its telemarketing activities. Its 'cold

11 Telephone subscribers can have their preference not to be contacted by direct marketers recorded on the National Directory Database (NDD) by contacting their line provider who will supply the relevant details to the NDD.

calling' marketing campaign had been suspended for a total of twenty days as a result of the actions taken by my Office.

This case demonstrates that my Office will take strong and effective action, such as requiring the suspension of marketing activities, where necessary. Complaints about telemarketing from the general public are an indicator of problems in the procedures or systems in companies which operate in the telemarketing sector. My Office continues to ensure that those companies complained of take immediate steps to identify the problems and then sort them out without delay. If the suspension of a company's marketing activities is necessary to achieve corrective measures, we will not hesitate to require such action, difficult though it may be for the company concerned.

Case Study 5: Excessive Personal Data on EU Single Payment Scheme Application Forms

I received a complaint that the EU Single Payment Scheme Application Forms, which are issued annually by the Department of Agriculture, Fisheries & Food, contained pre-printed data in respect of the date of birth and PPS number of the farmers to whom the forms are issued. A farmer informed my Office that he, and many other farmers, would usually need to get professional assistance from Teagasc or other qualified agents in the completion of these forms. He pointed out that the pre-printing of this personal data on the forms infringed his privacy as he had no means to restrict his professional adviser from viewing his date of birth and PPS number. He also stated that it would be normal for those professional advisers to retain copies of the completed forms in case the Department of Agriculture & Food raised queries which might need to be referred back to the advisers at a later stage.

In contacting the Department on this matter, we highlighted that both PPS numbers and dates of birth constitute personal data and are, therefore, subject to the protections set down in the Data Protection Acts, 1988 and 2003. We went on to state that in a situation where the Department sends out forms with personal data pre-printed on them and is aware that the recipients may need the assistance of third parties to complete them, the Department must make every effort to ensure that only the very basic personal details - such as name and address - are pre-printed. We pointed out that the problem with pre-printing

other personal data is that it gives the recipient only one choice in terms of safeguarding it – that is that he/she could blacken it out or otherwise delete it prior to showing it to a third party. We expressed some doubt about whether the Department would welcome the return of completed application forms which were somewhat defaced. Finally, we drew attention to the potential risks to the privacy of an individual where their personal data, such as a PPS number, fell into the hands of a third party.

The Department examined the matter and it immediately set about taking into account the concerns which my Office had expressed. In the drafting of the Application Form for 2008, the Department commendably removed completely the data fields concerning the applicant's date of birth and PPS number.

This case demonstrates how common it is for public bodies or other authorities to fall into the practice of processing categories of personal data even where such data is not needed to administer the scheme or application in question. Greater care must be taken by all concerned to ensure that only the minimum amount of personal data necessary is processed in the administration of schemes run by public bodies. In particular, I strongly advise public bodies which are authorised to use PPS numbers to do so sparingly and with extreme care.

Case Study 6: Data Controller breaches data protection law in regard to use of covert CCTV footage

I received a complaint in October 2006 from a data subject regarding the unfair obtaining by her employer of her personal information and its subsequent use as evidence to terminate her employment. The data subject had been employed in a supervisory capacity at the Gresham Hotel in Dublin for a number of years. In January 2005 she was called to a meeting by hotel management, at which she was informed that covert cameras had been installed some time previously in the hotel for the purposes of an investigation. The investigation was initiated on foot of a complaint received by the hotel regarding cash handling at the bar. The data subject was not the subject of the investigation, she was not made aware of the investigation nor was she informed of the covert CCTV recordings. At the meeting, the data subject was confronted with a series of questions and was asked to explain some of her actions which had been recorded by the covert cameras. Later in 2005, she was dismissed from her employment with the hotel. Evidence taken from the covert CCTV recordings was used in the decision to terminate the data subject's employment. No criminal prosecutions took place following the hotel's investigation nor was the data subject interviewed by An Garda Síochána.

As part of the detailed investigation into this complaint, my Office initially sought the observations of The Gresham Hotel regarding this issue, drawing particular attention to the fair obtaining principle of the Data

Protection Acts 1988 & 2003. The use of recording mechanisms to obtain data without an individual's knowledge is generally unlawful. Such covert surveillance is normally only permitted on a case by case basis where the data is gathered for the purposes of preventing, detecting or investigating offences, or apprehending or prosecuting offenders. This provision automatically implies an actual involvement of An Garda Síochána or an intention to involve An Garda Síochána.

In response to our initial queries, the hotel stated that the cameras were installed for a legitimate and specified purpose - the investigation of a complaint regarding cash handling in this area. It stated that it was of the opinion that the processing of this information was necessary for the protection of a legitimate legal interest, the protection of property of the hotel in response to a specific concern it had. The hotel also emphasised in its early correspondence with my Office that at no point were the cameras hidden or covert and it presumed that all employees would have seen them.

During our investigation, the data subject supplied photographs of electrical type data boxes/sockets that were located in the bar area of the hotel as it was her understanding that the covert cameras were hidden within these boxes. My Office forwarded copies of these photographs to the hotel requesting clarification on the matter. In response it indicated that these electrical type data boxes were telephone connections, microphone connections and internet connections and were never used as a means to record images for CCTV footage.

As part of our investigation, my Office visited the Gresham Hotel for the purpose of viewing the CCTV footage in question and to inspect the area in which the CCTV footage had been recorded. During this inspection, as well as viewing the footage, we were shown two electrical type boxes located just below ceiling level in the bar area and these boxes were identified as having been the location for the covert cameras. The location of the boxes also matched the views of the bar area which could be seen in the CCTV footage. The boxes were marked "1" and "2" and they appeared to be the same as the electrical boxes which appeared in the photographs which were previously supplied by the data subject. This clearly conflicted with the earlier information which the hotel had supplied to my Office as part of its investigation. Following this inspection, my Office was satisfied, on the basis of all of the information which had been compiled during our investigation, that the data protection rights of the data subject had been breached. Covert CCTV cameras had been installed to investigate specific incidents. The data subject was not the subject matter of this investigation. The personal data of the persons captured on the footage was obtained for one purpose - the investigation of specific incidents in the hotel. In the case of this data subject, her personal data was further processed in a manner incompatible with the original purpose. Furthermore, the data subject's personal data was not processed in accordance with the requirements of 'fair processing' as she had not been informed by the data controller, at the time when the data controller first processed her data, of the purpose for which it intended to process her personal data.

As the Acts require me to try to arrange, within a reasonable time, for the amicable resolution by the parties concerned of the matter which is the subject of a complaint, my Office asked both parties to consider this approach. Within a few weeks, a settlement was agreed between the parties. I was pleased that my Office was able to close its investigation file on the basis that an amicable resolution had been reached.

Case Study 7: Aer Lingus - Disclosure of employee information

Early in 2007, my Office received a significant number of complaints from employees of Aer Lingus regarding an alleged disclosure of their personal information by Aer Lingus to a third party without their consent. According to the complainants, the Human Resources Division of Aer Lingus had passed on the names, staff numbers and place of employment of its staff to HSA Ireland without the knowledge or consent of the employees concerned. Staff of Aer Lingus had become aware of this matter when they received personally addressed promotional literature from HSA Ireland, a healthcare organisation offering a range of health care plans. In this promotional literature, a copy of which was received in my Office, HSA Ireland informed the Aer Lingus employees that Aer Lingus had agreed to allow it to directly distribute the information to them.

Section 2 of the Data Protection Acts, 1988 and 2003 sets out the position in relation to the collection, processing, keeping, use and disclosure of personal data. It provides that data should be obtained and processed fairly, kept for only one or more specified purposes and it should be used and disclosed only in ways compatible with that purpose or those purposes. It also provides that personal data should not be processed by a data controller unless at least one of a number of conditions is met - one of those conditions being the consent of the data subject to the processing.

In response to initial contact from my Office regarding the alleged disclosure of personal information, Aer Lingus confirmed that it had passed on the personal data of its staff to HSA Ireland and it set out the background to how it had occurred. It explained that the company had previously operated and administered a Staff Welfare Fund to assist employees in certain circumstances in relation to personal and family medical expenses. As this fund had closed, Aer Lingus committed to putting another scheme in place and it negotiated with HSA Ireland to offer a replacement scheme to employees. In order to increase staff awareness of this new scheme, it was decided that it would be in the best interests of staff to write to them directly at their place of employment. Employee names and staff numbers were provided to HSA Ireland by means of a mail merge file. Aer Lingus was of the opinion that this disclosure was legitimate in accordance with what it regarded as a bona fide employment purpose. It also confirmed that consent had not been sought or obtained from its employees prior to the forwarding of the employee details to HSA Ireland.

My Office reminded Aer Lingus of its obligations under Section 2 of the Data Protection Acts with regard to the processing of personal data and it pointed out that the personal data of its staff should not have been disclosed to a third party without the consent of the employees concerned. In the circumstances, my Office sought and obtained confirmation from Aer Lingus that it had now destroyed the mail merge file containing the names and staff numbers which it had forwarded to HSA Ireland. Confirmation was also received from HSA Ireland that it had not retained records of Aer Lingus employee names, addresses, payroll or payslip numbers on any database.

My Office was satisfied by the steps taken by Aer Lingus and HSA Ireland in terms of corrective action. By way of clarification, we pointed out that the key issue from a data protection perspective was that Aer Lingus had facilitated contact from a third party to its employees concerning the availability of a staff welfare scheme while the same information could have been promulgated to those employees without raising any data protection concerns had Aer Lingus sent it directly to its employees instead.

I fully recognise that employers may, from time to time, wish to communicate details of various schemes to their employees. This can easily be achieved without infringing on the data protection rights of employees if the employer supplies the information directly to its employees or by some other means in conformity with the Data Protection Acts. My Office had only in the weeks before these complaints were received conducted an audit of Aer Lingus which had generally found a high level of compliance with data protection requirements. The occasion of the audit could have been used to seek advice from my Office on this issue.

My Office is always available to give advice to data controllers and the public alike in relation to data protection responsibilities and rights.

Case Study 8: Failure to finalise a complaint against Money Corp Limited

I received a complaint from a data subject in February 2007 regarding the failure of Money Corp Limited to respond to an access request made by him in November 2006. The right of access to personal data is one of the key fundamental rights conferred on a data subject by the Data Protection Acts. The Acts provide that access requests must be complied with by a data controller "as soon as may be and in any event not more than 40 days" after receipt of the request. My Office commenced an investigation which lasted for a period of some seven months.

During our investigation, we received correspondence from a firm of Dublin-based solicitors acting for Money Corp Limited stating that its client had responded to the data subject's access request in early May 2007. However, the data subject subsequently informed us that some critical documents had not been included in the response he had received to his access request. Accordingly, our investigation continued on the basis that Money Corp appeared to have failed to comply in full with the data subject's access request. We communicated further with Money Corp's solicitors regarding the matter of the outstanding documents.

At the end of August 2007, my Office received correspondence from these solicitors in which they stated that their client had furnished the data subject with any documentation held by them. They went on to state that their client's instructions were that any further documentation that the data subject considered to be outstanding "must have been mislaid during the process of moving offices as they have moved offices three times in the intervening period." The solicitors concluded their letter by informing my Office that all further correspondence on this matter should be directed to the registered office of Money Corp Limited.

My Office was very concerned at this turn of events and it was particularly cognisant of the fact that the outstanding documents could be of considerable importance to the data subject in relation to proving outstanding financial matters of a very significant nature. Accordingly, in order to investigate the matter further, one of my authorised officers, using the powers conferred by Section 24 of the Data Protection Acts, visited an address in Dun Laoghaire, Co. Dublin at which the company was registered with the Irish Financial Services Regulatory Authority (We had previously found out that the company was not trading at the address at which it was registered with the Companies Registration Office). Despite three separate attempts to gain access to the premises in Dun Laoghaire, the authorised officer failed to gain access or to make contact with any member of staff of Money Corp at the premises. Following this, my Office communicated again with the solicitors for Money Corp to which we subsequently received a reply which stated that "we have been unable to obtain further instructions from our client and we are now closing our file. As a result, we will be no longer representing them in relation to this matter."

By way of a further attempt to communicate with Money Corp Ltd, my Office sent a letter by registered post in early October 2007 to the company's Dun Laoghaire address. This letter was returned by An Post to my Office in November 2007 with an indication from An Post that nobody was available at the address on the delivery date and that it was not subsequently collected at the mail centre.

Unfortunately, despite extensive efforts by my Office to make direct contact with Money Corp Limited, we were unable to do so. As our investigation was effectively stymied, we found ourselves in the unsatisfactory situation of being unable to pursue the complaint to finality, despite the best possible use of the powers available to me. In the circumstances, my Office has communicated with the Financial Regulator in relation to the details of this case.

Case Study 9: Marketing Calls by Eircom - remedial action - amicable resolution.

During the first half of 2007 I received a large number of complaints from members of the public who had received marketing telephone calls from a telecommunications company, Eircom. Many of the complaints came from people who were ex-customers of Eircom and the marketing calls from the company were made in an effort to win back their business. Some of these complainants informed Eircom that they did not wish to receive further marketing calls but the company continued to call them. Others had their phone numbers listed on the National Directory Database (NDD) opt-out register but continued to receive marketing calls from Eircom.

Regulation 13 (4) of Statutory Instrument 535 of 2003 prohibits the making of an unsolicited telephone call for marketing purposes to the line of a subscriber where the subscriber has notified the person or company making the marketing call that he/she does not consent to the receipt of such a call on his/her telephone line or where the subscriber has had his/her telephone number recorded in the NDD opt-out register. It is an offence to make a marketing call which breaches this Regulation.

My Office investigated the complaints and engaged at length with Eircom on the matter. This involved meetings with the company as well as several exchanges of correspondence which eventually led to the following favourable and positive outcome from my perspective:

- Eircom assured me that it is fully committed to ensuring compliance with data protection legislation within the organisation.
- It expressed concern about the complaints received by my Office and it assured me that it takes all such complaints very seriously.
- Eircom introduced a number of measures to reduce the risk of any reoccurrence of such complaints. These measures involved the completion of a full internal review of the processes which are followed by all customer-facing channels when recording requests to opt-out of direct marketing by Eircom and its related companies. Where any points of weakness within these processes were identified, the process was revised to ensure that it was both robust and compliant with data protection legislation.
- Eircom briefed all relevant staff on the issues which gave rise to complaints and on the new processes which were put in place. The new processes also became an integral part of the training material for new staff.
- Eircom established a centralised and dedicated 'suppression' unit with responsibility for processing "do not call" requests received by post, email or fax.
- A statement was placed on Eircom's Intranet homepage emphasising the importance of ensuring compliance with data protection rules. The statement also explains the process which must be followed to implement a suppression request (i.e. an individual's stated preference not to be called by the company for marketing purposes) and it provides details of the new centralised 'suppression' unit.
- Eircom conveyed its sincere apologies to the complainants to my Office for any inconvenience caused to them and it entered the complainants' contact details on its suppression list to prohibit further marketing calls from the company to those individuals.
- In order to demonstrate its commitment to the protection of individuals' data protection rights and its regret for the issues which gave rise to complaints to my Office, Eircom made a donation of €35,000 to a reputable Irish charity.
- Finally, following agreement with my Office on the content, Eircom published a statement on its website regarding the protection of customer information. In the statement, among other things, Eircom acknowledged that it had communicated with individuals whose preference to decline marketing contact was not recorded due to a problem with its systems and processes and it expressed regret that these people were contacted when they did not want to be. It also stated that it had identified areas for improvement and had implemented those improvements.

Overall, I am very pleased with the investigation of these complaints and the steps taken by Eircom in response to my Office's intervention. The complainants concerned had good reason to complain to my Office about unsolicited marketing telephone calls which have become, in recent years, an all-too-frequent intrusion into the personal lives of individuals in their homes. Eircom identified the failings in its marketing processes and it did what a responsible data controller should do in similar circumstances - it took effective

remedial action. In addition, it responded positively to my Office's efforts to amicably resolve the complaints - the Data Protection Acts make provision for the amicable resolution of complaints in the first instance between the parties concerned - by apologising to the complainants and by making a substantial donation to charity. Furthermore, I am happy to report that since Eircom took the remedial steps outlined above I have received no further complaints of substance regarding its marketing activities.

Case Study 10: Member of staff at Revenue accessing and using personal data of a taxpayer

In January 2007, I received a complaint from a data subject who claimed to have been harassed by the receipt of a large number of anonymous text messages on her mobile phone. Among other things, the text messages referred to various details of personal information related to the data subject and personal information of some of her family members. Prior to referring the matter to my Office, the data subject informed me that she had made a complaint to An Garda Síochána about this matter. She claimed that the Gardaí traced the sender's number to a particular person to whom she had once been introduced very briefly. The data subject alleged that the sender, who was employed by the Revenue Commissioners, had obtained her personal information and that of her family members by accessing personal files held by the Revenue Commissioners.

My Office began an investigation of this complaint by contacting the Revenue Commissioners. We asked that the audit trail of the relevant files of the individuals concerned be examined to determine if they had been accessed by any staff member who did not have a legitimate business reason for doing so.

Following a prolonged examination, the Revenue Commissioners confirmed in June 2007 that it had been ascertained that one of its officers had accessed the records of the data subject and members of her family during the period November 2006 to February 2007, that such access was not part of the officer's

official duties and that it would appear that information gained from this access was passed to third parties unknown. The Revenue Commissioners stated that the matter was being dealt with by its Personnel Branch under the Civil Service Disciplinary Code. It went on to state that it was seriously concerned about any instances of unauthorised access by its staff to taxpayer data held on its computer systems and that appropriate disciplinary action had been taken and would continue to be taken in individual cases.

Some time later, the Revenue Commissioners issued a letter to the data subject in which it acknowledged that her records and those of her family had been accessed by one of its officers and that the access was not part of the officer's official duties. The letter sincerely apologised to the data subject for the inappropriate accessing of her records and those of members of her family and it expressed deep regret that this occurred.

I regard this case as a very serious matter. A large amount of personal information is entrusted to the Office of the Revenue Commissioners which has a responsibility to ensure that it is kept safe and secure. A minimum standard of security for such information would include, among other things, that access was restricted to authorised staff on a 'need to know' basis. In this case, it emerged that the staff member who accessed the information had no legitimate business in doing so. That staff member abused a position of trust and proceeded to access and use personal information unlawfully. I will await with keen interest the outcome of the disciplinary proceedings which the Revenue Commissioners have commenced under the Civil Service Disciplinary Code in connection with this matter.

Case Study 11: Croke Park - Retention of personal data of nearby residents

In July 2006 I received a complaint from a data subject regarding the retention, use and security of personal data collected by Páirc an Chrócaigh Teoranta (Croke Park Stadium).

The complaint came about as a result of a letter which the Stadium Director at Croke Park had issued to residents in the area in relation to the setting up of a database through which the residents would be considered for tickets to some of the events held in Croke Park. In this letter, the Stadium Director stated that he was very conscious of the fact that Croke Park was situated in a residential area and was part of the local community. He pointed out that Croke Park had, in recent years, looked at ways of making some tickets available to the community for different events. It had now decided to introduce a new scheme involving the setting up of a database of people living in the area which would help ensure that tickets, when they were available, went to the right people. In order to be considered for tickets, interested residents were required to complete an application form and submit some form of photo identification, such as a passport or driving licence, as well as a utility bill. The data subject had serious concerns in relation to the type of information which was sought, how it was going to be used and the security surrounding the holding of the data.

My Office contacted Croke Park to raise the issues in the complaint and to make it aware of its obligations under section 2 of the Acts which provides, among other things, that data shall be processed fairly, kept for only one or more specified purpose, kept safe and secure and that it shall be adequate, relevant and not excessive. Croke Park responded in detail in relation to the data protection issues my Office raised and stated that the information would not be disclosed to any third parties and would not be used for any purpose other than to notify residents when tickets would be made available to them. It also informed my Office of the security measures it had in place to keep the data safe and secure. In relation to the extent of some of the personal information sought, Croke Park responded by saying that it had a legitimate concern to ensure that identities and home addresses were verified correctly and it stated that an annual audit would ensure that all out-of-date information was deleted.

My Office remained concerned that the residents were not made aware of how their data would be used by Croke Park and we suggested that this could be done through the inclusion of a data protection notice in the renewal letter which issues to all residents annually. We also had concerns regarding the retention of identity documents and we informed Croke Park that data controllers should not retain copies of personal data such as passports, driving licences and utility bills unless they had a statutory basis for doing so. My Office recommended that the residents be allowed to present their identification in person to Croke Park or alternatively, in relation to documents submitted by post, that Croke Park undertake to return the identification documents uncopied to the residents once verified. Croke Park took my Office's recommendations on board and agreed to amend all future application forms to include a data protection notice. It also agreed to return all copies of identification and utility bills to those residents who had already submitted application forms to Croke Park.

I was satisfied that Croke Park took its responsibilities as a data controller seriously and I was encouraged by the prompt manner in which it addressed the issues raised by my Office by revising its procedures to take into account the data protection rights of the individuals involved.

Increasingly my Office is being informed of circumstances where data controllers retain copies of personal information used for identification purposes. Without a statutory basis for retaining copies of such documents, a data controller has no entitlement to keep a copy on file. There is no impediment to requesting sight of identification documents in order for a data controller to satisfy itself of a data subject's identity and a system for doing this can be put in place without too much effort.

Case Study 12: Biometrics in the workplace - need for staff consent

I received a number of complaints from staff employed at a logistics company in relation to the proposed introduction of a biometric system at that company for the purpose of time and attendance. These staff considered that their data protection rights would be infringed by being required to provide their employer with a fingerprint. The use of a biometric system impacts on several data protection principles including proportionality, fair obtaining, accuracy and security of personal data.

My Office commenced its investigation by contacting the company and referring it to the extensive guidelines on our website in relation to biometrics in the workplace. During our investigation, a meeting was held with a representative of the company to discuss the matter. In a privacy impact assessment, the company outlined its reasons for the introduction of the biometric system as health and safety, security, administration and cost effectiveness. It also provided details of the type of biometric system it intended to use - a touch verification system. The system requires a fingertip to be inserted into a reader which converts the fingertip into an encrypted algorithm and then the employee enters their unique pin number onto a pad. The system then stores a numeric sequence on a central database. It was claimed that the numeric sequence cannot be reversed or used for any other purpose except for verification and it is also encrypted.

The company also stated that it had looked into other forms of recording time and attendance and found that the biometric system would be the most efficient and cost effective. It also said that other systems could possibly be open to abuse. It stated that it had, in the past, experienced problems regarding abuse in relation to recording attendance. It also assured my Office that all employees, except for the staff who complained to my Office, had consented to the use of the touch verification system. The company said that it had held information sessions in each of its company branches and that written documentation and training had been given to all employees. Any employees who had objections to the system or wanted more information were also invited to address these with management. It also confirmed that the staff who complained to my Office had not been required to start using the system.

The approach of my Office is to try to understand the circumstances that lead a particular data controller to introduce a biometric system using the personal data of its employees, bearing in mind that the scan of a fingerprint is personal data even if converted into an algorithm. My Office reviewed the privacy impact assessment submitted in this case and the company's responses to our queries. Taking into account the company's cooperation in the matter, it was agreed that the staff concerned should use a pin code system rather than the biometric system for recording time and attendance. This would not give rise to any issues under the Data Protection Acts. Furthermore, these staff would not be required to use the biometric system in the future, without the company first taking the matter up with my Office. On that basis, I was happy

to conclude the matter given that the issues raised by the individuals who made the complaints to my Office had been addressed. I was satisfied that the company had not breached the data protection rights of those staff as it had not required them to use the biometric system against their wishes.

Case Study 13: Dairygold - Failure to comply in full with an Access Request

In June 2006, I received a complaint from a firm of solicitors acting on behalf of a client regarding alleged non-compliance with a subject access request. The data subject had made an access request to her employer, Dairygold Co-Operative Society Limited/ REOX, in March 2006 but it had not been complied with within the statutory forty day period.

My Office wrote to the data controller and we subsequently received a reply to the effect that the material sought in the access request had now been supplied. However, following examination of the documents received, the solicitor for the data subject communicated further with my Office and identified certain documents omitted by the data controller. Particular reference was made to documents in relation to a workplace accident in which the data subject was involved in October 2004. My Office contacted Dairygold/Reox seeking an explanation for the missing documents. While it responded by providing observations on a number of the missing documents, it also stated that it was obtaining legal advice regarding the release of the documents relating to the workplace accident.

After the exchange of detailed correspondence between my Office, Dairygold/Reox and its legal representatives, an index of all of the personal information which had been released was provided to my Office. In relation to the documents concerning the workplace accident, the solicitors for the data

controller confirmed that their client was in possession of both an Internal Accident Report and a Consulting Engineer's Report. It stated that both documents were prepared in contemplation of a personal injury claim and were therefore privileged.

To satisfy ourselves that there was a sound basis for the legal privilege claim in relation to these documents, my Office sought information from the data controller regarding the dates on which the two reports were created. It was confirmed that the Internal Accident Report Form was created in the days immediately following the workplace accident and the Consulting Engineers Report was created some nineteen months later in May 2006. My Office pointed out to the data controller's solicitor that the claim of legal privilege related only to communications between a client and his professional legal advisers or between those advisers and that this provision could not be applied to the internal accident report created shortly after the incident. In light of the information available to my Office, we accepted that the claim of legal privilege could be applied to the Consulting Engineer's Report. The data controller continued, however, to claim legal privilege on both documents. In an attempt to bring closure to this matter, my Office requested a confidential sighting of the Internal Accident Report. Regrettably, the data controller refused to comply with this request and I had no option but to serve an Information Notice requiring that a copy of the Internal Accident Report be furnished to me. The Internal Accident Report was supplied to me in response to the Information Notice. On examining the Report I was satisfied that it contained personal data of the data subject and I was further satisfied that the limited exemptions to the right of access set down in the Acts did not apply to this document. The document also contained some limited personal data of third parties and non personal information which we advised the data controller to redact with the balance to be released voluntarily to the data subject. The Report was subsequently released in accordance with our advice.

There is a tendency for data controllers in some cases to claim non-relevant exemptions under Sections 4 or 5 of the Acts to restrict the right of access. With increased frequency, accident reports in relation to workplace incidents are being withheld with data controllers claiming legal privilege on such reports. I do not accept that legal privilege applies to such reports. It is standard procedure for an accident report to be compiled by an employer in the aftermath of a workplace accident and such reports clearly do not fall into the category of personal data in respect of which a claim of legal privilege could be maintained in a court in relation to communications between a client and his professional legal advisers or between those advisers. Any data controller who is reported to me as having restricted a data subject's right of access to reports of this nature will face an investigation by my Office involving a close scrutiny of the grounds for applying the restriction. I will have no hesitation in using my full enforcement powers to ensure the rights of the data subject are upheld in relation to such cases.

Case Study 14: Ryanair - Remedial action taken for customers to unsubscribe from marketing

I received a complaint in September 2007 from a data subject who was finding it difficult to unsubscribe from the receipt of marketing material from Ryanair. She had booked a flight with the airline previously and had opted-in to the receipt of marketing material but she had now changed her mind and wanted to opt-out from Ryanair's marketing database. The data subject sent me copies of some of the marketing material which she had received by email from the company as well as copies of her attempts to unsubscribe by email to Ryanair.

On examining the matter closely, my Office found that Ryanair had provided an opt-out facility at the end of its marketing email messages, as marketers are required to do under Regulation 13(7) of SI 535 of 2003. It invited recipients who wished to unsubscribe to send a blank email to an email address which began with the word 'leave' and which consisted of a string of over seventy characters comprising a varied mix of letters and digits. The data subject, in this case, had failed to unsubscribe as she had not realised that the word 'leave' formed part of the email address. In my view, this was a mistake which could easily be made as the text used in the unsubscribe section of Ryanair's email was not entirely clear and it provided no advice to customers.

Regulation 13(7) of SI 535 also requires marketers to provide customers with an opportunity to object to the receipt of further marketing in an easy manner. My Office asked Ryanair to explain how the provision of such a complex email address could be regarded as an easy manner of unsubscribing from its marketing database. The company, in reply, indicated that normally people 'copy and paste' the email address into a replying email. It also informed my Office that when a customer successfully submits an unsubscribe request, Ryanair sends back an email to the customer asking them to confirm by return email that they wished to unsubscribe. In effect, the company required customers to send two emails in order to unsubscribe. My Office noted that customers were not given any advice to the effect that they should copy and paste the email address in order to successfully submit the original unsubscribe email to the company nor were they advised that they would be required to submit a follow-up confirmation email. In the circumstances, we considered that customers had not been given an opportunity to opt-out in an easy manner and we asked Ryanair to take immediate steps to introduce a more user-friendly and easy unsubscribe facility for all recipients of its email marketing communications.

I am happy to report that Ryanair cooperated fully with my Office's investigation of this complaint and it promptly took on board our concerns regarding the opt-out facility. We subsequently received confirmation from the company that it had simplified the unsubscribe process by providing a link in the marketing email which the customer could simply click on to unsubscribe without the need to enter the long email address. It also removed the requirement for a customer to submit a follow-up email to confirm their wish to unsubscribe. These changes significantly eased the process of unsubscribing from Ryanair's marketing database and I welcome them.

The legitimate marketing of customers through the use of email is a common practice, if somewhat devalued by the sheer volume of such material which individuals receive. It is critical that marketers who use this tool comply fully with the requirements of SI 535 of 2003. This case shows the need for marketers to provide an opt-out facility on each marketing message which is simple and easy to use. It is my firm position that customers should not be required to send more than one email to a marketer in order to unsubscribe from that marketer's database. Any additional requirements placed on customers are unacceptable and contravene Regulation 13(7) of SI 535.

Case Study 15: On-line shoppers receive unsolicited marketing from Tesco

I received complaints from individuals regarding direct marketing emails which they had received from Tesco. In all cases, the complainants had registered for on-line shopping with Tesco. Soon afterwards they began receiving direct marketing emails. Before complaining to my Office the individuals had tried to unsubscribe from Tesco's marketing list by using the 'unsubscribe' facility provided in the marketing email. Despite their attempts to unsubscribe they continued to receive further marketing emails.

The legal requirements concerning the use of electronic mail for directing marketing purposes is set out in SI 535 of 2003. Marketers may send email for direct marketing purposes to an individual subscriber where:

a) they have obtained that subscriber's contact details in the course of a sale of a product or service to him/her;

b) the direct marketing material they are sending is in respect of their similar products and services;

and

c) during every communication, the subscriber is given a simple, cost-free means of refusing the use of his/her contact details for marketing purposes.

The 'unsubscribe' facility provided by Tesco to its customers failed in this instance and the individuals concerned continued to receive unwanted marketing material in contravention of the legal requirement.

My Office investigated the matter with Tesco and we sought immediately to have the email addresses of the complainants removed from the company's marketing database. We also asked for an explanation for the failure of the 'unsubscribe' facility. Tesco initially responded by advising that the email addresses of the complainants had been removed from the marketing lists at our request. Despite this assurance, the complainants continued to receive further direct marketing emails from the company. My Office informed Tesco of our disappointment with this turn of events and we stated that these latest breaches demonstrated a serious deficiency in the capacity of the company's marketing system to respect out-out preferences. We asked Tesco to seriously consider steps to amicably resolve the complaints.

Tesco further investigated the matter and found an issue with one of the methods that customers use to unsubscribe from its marketing emails. It immediately set about fixing the issue and while this was being done it directed customers to visit the website directly to unsubscribe. With regard to the previous assurance given that the individual complainants had been unsubscribed at the request of my Office, Tesco found that an error had been made in the manual process involved in unsubscribing them from the database. It corrected this error immediately. In light of the inconvenience caused, Tesco apologised to the individuals concerned and offered each of them gift vouchers as a goodwill gesture. This was accepted as an amicable resolution of their complaints. I was satisfied with the steps taken by Tesco to resolve this matter to the satisfaction of all concerned.

Marketers have a responsibility to ensure that their systems are continuously capable of unsubscribing those customers who wish to record such a preference in response to the receipt of a marketing email or text message. In that regard, I recommend that regular testing be carried out to ensure that the opt-out facility is functioning without fault. Ideally, such testing should be incorporated as a standard procedure in advance of scheduled marketing campaigns.

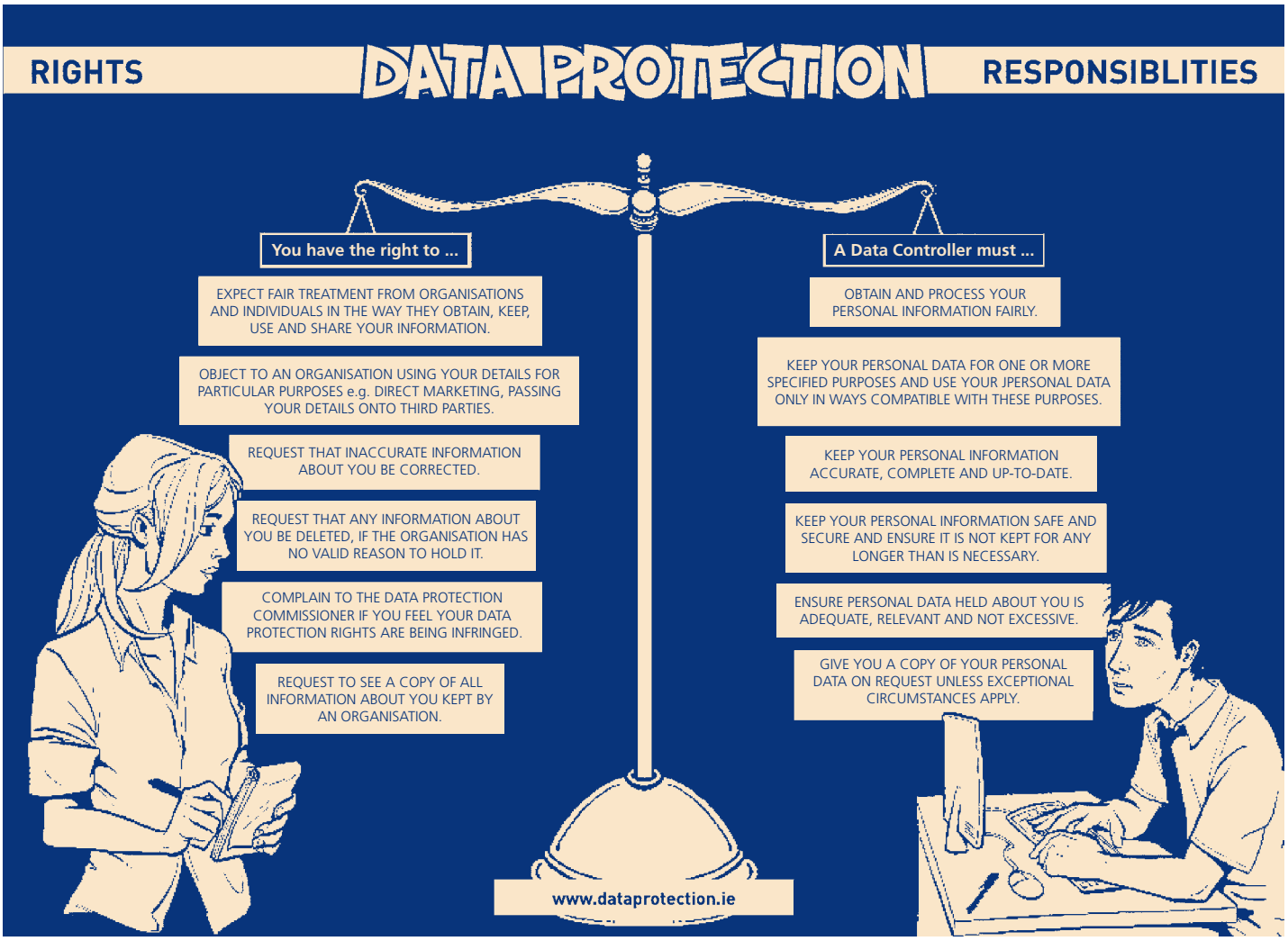
RIGHTS AND RESPONSIBILITIES

Rights of Data Subjects

Individuals (data subjects) are often requested to provide personal information about themselves to a variety of organisations and individuals (data controllers) for a whole range of purposes on a daily basis.

Responsibilities of Data Controllers

Data Controllers (organisation and individuals) collect personal information about individual data subjects.



Copies of this chart are available from the Office of the Data Protection Commissioner on request

PART 3 – GUIDANCE

Guidelines in relation to legal basis for private sector sharing of personal data

This note is seeking to give guidance in relation to the sharing of personal data in relation to individuals from data controller to data controller in the private sector. It is prepared in recognition of an increasing desire on the part of some data controllers to consider sharing personal data collected for one primary purpose such as providing a service to an individual for another purpose such as entering the personal data of that person on an industry wide database or other such broader database.

The sharing of data in relation to individuals, even with their consent, must still meet the requirements of the Data Protection Acts for justification for the particular processing envisaged.

All processing of personal data must be in compliance with the provisions of Sections 2 & 2A and where the data is sensitive Section 2B of the Data Protection Acts. In essence, this legal basis requires that personal data only be processed where it is necessary to do so for a substantial reason in the particular circumstances. Even in such circumstances all processing must still be carried out in such a manner as to safeguard the fundamental rights and freedoms of the individual concerned.

The key issue to be decided in the context of any processing of personal data is to establish under which of the provisions in Sections 2, 2A & 2B (where the processing relates to sensitive data) can the processing be deemed legitimate. Sharing of personal data is considered to be processing and therefore must have an appropriate basis in the Data Protection Acts.

Section 2

As a minimum to ensure fair processing, the person must be appropriately informed in accordance with the requirements of Section 2(1)a of the Acts as outlined in more detail in Section 2D. This requires that the persons must be informed as to all uses that will be made of their data including to whom it will be disclosed.

Section 2A

Once appropriate and detailed information is supplied to all persons under the requirements of Section 2(1)(a) of the Acts, the additional conditions of Section 2A must also be met. Section 2A(1) relates to consent. Where this consent is sought as a condition for the provision of the service in question rather than on a purely optional basis, then the strong view of the Commissioner is that it is doubtful that it can be considered to be freely given and therefore should not normally be solely relied upon as a justification for the sharing of personal data. This is especially so where such sharing is on a systematic, routine basis.

In such circumstances, one of the other conditions of Section 2A must also be met. The most likely in relation to the sharing of personal data is Section 2A(1)(d):

(d) *the processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party or parties to whom the data are*

disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the fundamental rights and freedoms or legitimate interests of the data subject.

Accordingly, any sharing of personal data would need to be able to clearly demonstrate that it is necessary for the legitimate interests of the data controller concerned and not prejudice the fundamental rights and freedoms or legitimate interests of the data subject. Therefore this provision requires that any sharing strike a clear balance between the interests of the data controller and the data subject. The strong view of the Data Protection Commissioner is that in order to override the legitimate interests of the data subject, the data controller must be able to demonstrate unequivocally why it is necessary for their legitimate interests to override the rights of individuals by sharing their personal data with others.

Section 2B

Additionally, where the personal data to be shared relates to the "the commission or alleged commission of any offence by the data subject" which would, of course, include fraud, it would constitute sensitive personal data and the conditions of Section 2B of the Acts also need to be met before any sharing of personal data takes place.

Section 2B again envisages the explicit consent of the data subject providing a basis for the processing of personal data under this Section. However, for the reasons outlined above a consent given in these circumstances should not normally be considered to be freely given and so cannot be solely relied upon by a data controller.

Section 2B(1) outlines additional conditions which would legitimise such processing. The most relevant in this context are likely to be:
(vi) the processing is necessary -
(1) for the administration of justice,
(11) for the performance of a function conferred on a person by or under an enactment, or
(111) for the performance of a function of the Government or a Minister of the Government,

(vii) the processing –
(I) is required for the purpose of obtaining legal advice or for the purposes of, or in connection with, legal proceedings or prospective legal proceedings, or
(II) is otherwise necessary for the purposes of establishing, exercising or defending legal rights

This makes clear that sensitive personal data in relation to the commission or alleged commission of an offence may only be processed by a data controller itself for the purpose of pursuing legal action or where the processing is performed further to a specific statutory obligation or for the administration of Justice. These latter categories may only be carried out by an official authority. Accordingly, for clarity, the sharing of personal data by a data controller with An Garda Síochána in relation to the commission or alleged commission of an offence is legitimate under the Acts and may take place. No other sharing of information between data controllers in relation to the commission or alleged commission of offences, including in relation to fraud, may take place in compliance with the Data Protection Acts.

Guidance Note for Electronic Communications Service Providers on direct marketing telephone calls to their Subscribers and former Subscribers.

Set out below is the position of the Office of the Data Protection Commissioner on direct marketing telephone calls by Electronic Communications Service Providers to their Subscribers and former Subscribers. This position is based on the legislative requirements concerning unsolicited communications as set down in S.I. No. 535 of 2003 - European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2003 and in Sections 2(7) and 2(8) of the Data Protection Acts, 1988 and 2003.

Subscribers to one telecommunications company for a single billing service.

This relates to subscribers who receive both call and line rental services from one telecommunications company (service provider). In such cases, the service provider who is currently supplying the service may telephone the line of their subscribers for direct marketing purposes such as alternative tariff plans, additional value-added services, etc. The NDD opt-out preference does not apply in such cases. However, the wishes of any subscriber who has indicated whether orally or in writing to their current single billing service provider that they do not wish to receive marketing calls must be respected and they may not, therefore, be telephoned for such calls once they have indicated such a preference. Furthermore, all other service providers must respect the NDD opt-out preference (if expressed) of non-customers (who are single billing subscribers of a different service provider) in relation to direct marketing telephone calls. An opt-out preference indication in the NDD must always be respected by such service providers unless the particular service provider can credibly demonstrate that it has obtained a separate clear direct marketing consent directly from the subscriber in question. A particular point arises in respect of single billing service subscribers who have terminated a business relationship with one or more previous service providers. In such circumstances, any opt-ins for direct marketing which were previously given to those service providers prior to the termination of the business relationship will be presumed to be expired.

Subscribers to carrier pre-selection services.

This describes a subscriber who opts in advance for certain types of calls (International, National, All calls) to be carried by one or more service providers. In such cases, service providers who are providing the pre-selection services may telephone the line of their current subscribers for direct marketing purposes such as alternative tariff plans, additional value-

added services, etc. The NDD opt-out preference does not apply in such cases. However, the wishes of any subscriber who has indicated whether orally or in writing to their service provider that they do not wish to receive marketing calls must be respected and they may not, therefore, be telephoned for such calls once they have indicated such a preference. Furthermore, all other service providers must respect the NDD opt-out preference (if expressed) of non-customers (who are carrier pre-selection subscribers of different service provider(s)) in relation to direct marketing telephone calls. Equally, the line rental service provider and/or ancillary services provider (services relating to the line rather than to calls, e.g. ISDN or CPS rental) must respect the NDD opt-out preference (if expressed) of such subscribers in relation to direct marketing calls for all services other than line rental service and/or the ancillary services in question as well as the wishes of any such subscriber who has indicated to their line rental and/or ancillary services provider that they do not wish to receive marketing calls. An opt-out preference indication in the NDD must always be respected by such service providers unless the particular service provider can credibly demonstrate that it has obtained a separate clear direct marketing consent directly from the subscriber in question.

Subscribers to carrier selection services.

This relates to subscribers who opt on a call-by-call basis for certain types of call (International, National, etc) to be carried by one or more service providers. In such cases, service providers who are currently providing the carrier selection services may telephone the line of their current subscribers for direct marketing purposes such as alternative tariff plans, additional value-added services, etc. The NDD opt-out preference does not apply in such cases. However, the wishes of any subscriber who has indicated whether orally or in writing to their service provider that they do not wish to receive marketing calls must be respected and they may not, therefore, be telephoned for such calls once they have indicated such a preference. Furthermore, all other service providers must respect the NDD opt-out preference (if expressed) of non-customers (who are carrier selection subscribers of different service provider(s)) in relation to direct marketing telephone calls. Equally, the line rental service provider and/or ancillary services provider must respect the NDD opt-out preference (if expressed) of such subscribers in relation to direct marketing calls for all services other than line rental service and/or the ancillary services in question as well as the wishes of any such subscriber who has indicated to their line rental and/or ancillary services provider that they do not wish to receive marketing calls. An opt-out preference indication in the NDD must always be respected by such service providers unless the particular service provider can credibly demonstrate that it has obtained a separate clear direct marketing consent directly from the subscriber in question.

Subscribers who change telecommunications company.

This relates to (i) subscribers who terminate their existing contract with their telecommunications service provider for both call and line rental services and (ii) subscribers who terminate their existing contract with their telecommunications service provider for carrier pre-selection or carrier selection services (as described above) where such services were the only services that were availed of by the subscriber from that service provider. Such termination of contract brings subscribers into the category of former subscribers of the service provider in question. Consent given by a subscriber to a service provider prior to the termination of a business relationship for the receipt of direct marketing calls on his/her line will be presumed to be expired on the termination of the business relationship unless the consent was given on the clear and specific understanding that it would continue to apply in the event of the termination of the business relationship. In the case of these former subscribers, in respect of direct marketing calls, the NDD opt-out preference (if expressed) must be respected by their former service provider with immediate effect on the termination of the business relationship.

Guidance Note for Data Controllers on Purpose Limitation and Retention

The following guidance has been prepared as an aid to data controllers in the practical application of Section 2(1)(c) of the Data Protection Acts 1988 & 2003 which requires data controllers to comply with the following provisions concerning personal data kept by them:

- the data shall have been obtained for one or more specified, explicit and lawful purpose(s),
- the data shall not be further processed in a manner incompatible with that purpose or those purposes,
- the data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they were collected or are further processed, and
- the data shall not be kept for longer than is necessary for that purpose or those purposes.

Specific, explicit and lawful purposes

Data controllers who obtain personal data from a data subject may do so for one or more specific, lawful and clearly stated purposes. It is unlawful to collect information about people routinely and indiscriminately – a data controller must have a sound, clear and legitimate purpose for collecting personal data. An individual has a right to question the purpose for which you hold his/her data and you must be able to identify that purpose.

Further processing

Data controllers who obtain personal information for one or more legitimate purposes may not use that data for any other purpose except in ways which are compatible with the original purpose(s). For example, personal images captured on CCTV cameras by a data controller where the CCTV was in operation solely for security purposes may not be used by the data controller for any other purpose such as staff monitoring.

Similarly, telephone service providers hold personal information for the purpose of providing a telephone service to subscribers (and the associated functions of telephone billing, line repairs, etc). They may be obliged by law to retain traffic and location data for three years. In the event of a subscriber terminating his/her relationship with a telephone service provider, the service provider may not, for example, process the personal data of that subscriber (which the service provider may be lawfully required to retain), to target him/her in person, by post, electronically or otherwise with direct marketing material or visits by sales agents [in an effort to win-back their business]. The only exception is where, prior to the termination of the customer relationship, the customer has clearly opted in (as opposed to not having opted-out) to such contact taking place in the event of the termination of the business relationship. This guidance note updates the previous position of the Office of the Data Protection Commissioner on that matter.

In order to meet this obligation, data controllers are advised to put in place appropriate procedures and security measures to ensure that information obtained for one purpose may not be accessed and used for another purpose within their organisation. This will include audit trails, etc. to ensure that such unauthorised access, where it might take place, can be tracked and provide a basis for appropriate measures to be taken to deal with it.

Adequate, relevant and not excessive.

The personal data sought and kept by data controllers should be sufficient to enable them to achieve their specified purpose(s) and no more. Data controllers should set down specific criteria to judge what is adequate, relevant and not excessive and they should apply those criteria to each information item and the purpose(s) for which it is held. Data controllers have no basis for collecting or keeping personal data that they do not need on the off-chance that a use might be found for it at a future date.

Retention

Data controllers must be clear about the length of time for which personal data will be kept and the reasons why the information is being retained. In determining appropriate retention periods, regard must be had for any statutory obligations imposed on a data controller. If the purpose for which the information was obtained has ceased and the personal information is no longer

required, the data must be deleted or disposed of in a secure manner. It may also be anonymised to remove any personal data. In order to comply with this legal requirement, data controllers are advised to assign specific responsibility and introduce procedures for ensuring that files are regularly purged and that personal data is not retained any longer than is necessary.

Guidance Note on Biometrics in Schools, Colleges and other Educational Institutions

The following guidance has been prepared as an aid to schools, colleges and other educational institutions that may be considering the installation and use of a biometric system. This document is intended to encourage such institutions to fully consider if there is need for a biometric system in the first place and then to assess the privacy impact of different systems.

The critical issues to be considered from a data protection perspective are the proportionality of introducing a biometric system and the requirement to obtain the signed consent of the student users (and their parents or guardians in the case of minors) giving them a clear and unambiguous right to opt out of the system without penalty.

The document is not intended to promote any particular system, but is intended to make schools and colleges aware of their responsibilities under the Data Protection Acts 1988 & 2003. It is the use of a biometric system that may give rise to a data protection concern, not necessarily the production or sale of a system. All situations must be judged on a case-by-case basis.

1. Different types of Biometric systems

All biometric systems operate on the basis of the automatic identification or authentication/verification of a person. What differs between systems is the nature of the biometric and the type of storage.

1.1 Information used to generate biometric data

Biometric data may be created from physical or physiological characteristics of a person. These include a fingerprint, an iris, a retina, a face, outline of a hand, an ear shape, voice pattern, DNA, and body odour. Biometric data might also be created from behavioural data such as hand writing or keystroke analysis. Generally, a digitised template is produced from the biometric data. This template is then compared with one produced when a person presents at a reader.

1.2 Types of biometric data.

There are three principal types of biometric data:

- Raw Images, consisting of recognisable data such as an image of a face or a fingerprint, etc.
- Encrypted images, consisting of data that can be used to generate an image.
- Encrypted partial data, consisting of partial data from an image, which is encrypted and cannot be used to recreate the complete original image.

1.3 Types of Biometric systems

There are two principal types of systems:

- Identification systems, which confirm the identity of an individual;
- Authentication / verification systems, which confirm that a biometric derived from a person who presents at a reader matches another biometric, typically stored on a card and presented simultaneously.

1.4 Storage of biometric data.

There are two principal methods of storing biometric data/templates:

- Central databases store the templates on a central system which is then searched each time a person presents at a reader.
- A card is used to store a template. A template is generated when a person presents at a reader, and this template is compared with the template on the card.

Data Protection issues concerning biometrics.

2. Proportionality

Section 2(1)(c)(iii) of the Data Protection Acts states that data

"shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they were collected or are further processed."

The key word here is "excessive." Accordingly, the first question to be asked when considering the installation of such a system is what is the need for it? What is wrong with current systems or less invasive alternatives?

As individuals have fundamental Human Rights which are protected by the Data Protection Acts, a school or college must conduct some assessment of the need for a biometric system and an evaluation of the different types of available systems before the introduction of any particular system.

Determining what is excessive requires a case-by-case analysis. Some factors which may be taken into account include:

- **Environment.** Does the nature of the school or college require high levels of security? Are there areas of the campus which contain sensitive information, high value goods or potentially dangerous material which may warrant a higher level of security than would areas with low value goods or areas with full public access? Of course such a consideration would also point towards all persons working in the environment being similarly required to use the biometric system.
- **Purpose.** Can the intended purpose be achieved in a less intrusive way? A biometric system used to control access for security purposes in certain areas of the campus might be legitimate while a biometric system used by the same school or college purely for attendance management purposes might not.
- **Efficiency.** Ease of administration may necessitate the introduction of a system where other less invasive systems have failed, or proved to be prohibitively expensive to run.

- **Reliability.** If a school or college suffers as a result of students impersonating each other for various reasons, then a system could possibly be justified as long as other less invasive ones have been assessed and reasonably rejected.

3. Fair obtaining and processing.

Section 2(1)(a) of the Acts require that:
"The data or, as the case may be, the information constituting the data shall have been obtained, and the data shall be processed, fairly."

In order to demonstrate compliance with this provision, at least one of the provisions of Section 2A of the Acts must be met. In the context of the introduction of a biometric system for use by students in a school or college, these include:

- Consent, and
- Legitimate interests of the school or college: where the processing is necessary for the purposes of the legitimate interests pursued by the school or college or by a third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the fundamental rights and freedoms or legitimate interests of the data subject.

Consent: In the context of students attending a place of education, the Data Protection Commissioner would stipulate that the obtaining of consent is of paramount importance when consideration is being given to the introduction of a biometric system. It is the Commissioner's view that when dealing with personal data relating to minors, the standards of fairness in the obtaining and use of data, required by the Data Protection Acts, are much more onerous than when dealing with adults. Section 2A(1)(a) of the Data Protection Acts states that personal data shall not be processed by a data controller unless the data subject has given his/her consent to the processing, or if the data subject by reason of his/her physical or mental incapacity or age, is or is likely to be unable to appreciate the nature and effect of such consent, it is given by a parent or guardian etc. While the Data Protection Acts are not specific on what age a subject will be able to consent on their own behalf, it would be prudent to interpret the Acts in accordance with the Constitution. As a matter of Constitutional and family law a parent has rights and duties in relation to a child. The Commissioner considers that use of a minor's personal data cannot be legitimate unless accompanied by the clear signed consent of the child and of the child's parents or guardian.

As a general guide, a student aged eighteen or older should give consent themselves. A student aged from twelve up to and including seventeen should give consent themselves and, in addition, consent should also be obtained from the student's parent or guardian. In the case of children under the age of twelve, consent of a parent or guardian will suffice. All students (and/or their parents or guardians as set out above) should, therefore, be given a clear and unambiguous right to opt out of a biometric system without penalty. Furthermore, provision must be made for the withdrawal of consent which had previously been given.

Legitimate interests: Whilst the "legitimate interest" provision may seem appealing, it requires that a balance be struck. What is acceptable in one case may not be acceptable in another and a school or college seeking to rely upon this provision must take into account the potential effect upon student privacy rights. In any event, the Data Protection Commissioner considers that, in the context of a student environment, the processing of personal data using a biometric system would be prejudicial to the fundamental rights and freedoms of the students concerned in the absence of freely given consent.

3A. Fair obtaining of sensitive data.

If a biometric identifies sensitive data (such as data relating to a student's health or facial appearance thereby revealing race), at least one provision of section 2B of the Acts must be met in addition to those mentioned above. In the context of the introduction of a biometric system for use by students in a school or college, these provisions include:

- consent explicitly given.
- necessary processing for the performance of a function conferred on a person by or under an enactment.

Explicit consent: As stated above, all students (and/or their parents or guardians) should be given a clear and unambiguous right to opt out of a biometric system without penalty. The same consent which applied to the principle of obtaining and processing data fairly also applies to the fair obtaining of sensitive data.

Necessary for the performance of a function conferred under an enactment: Any legal obligation to record the attendance of students need not, in itself, require a biometric system to satisfy. For example, the Education (Welfare) Act, 2000 requires schools to maintain a record of the attendance or non-attendance on each school day of each student registered at the school. This requirement does not specify how the attendance data should be obtained. The key word in this provision of the Data Protection Acts concerning the processing of sensitive personal data is "necessary." It is the view of the Data Protection Commissioner that the processing of sensitive personal data through use of a biometric system is ***not necessary*** to meet the requirements of the Education (Welfare) Act, 2000 in respect of recording student attendance. There are several long established and successful alternative methods of recording student attendance at schools which do not require the processing of a student's sensitive personal data.

4. Transparency

Section 2D of the Acts require that a school or college provide at least the following information to students when processing their data:

- The identity of the data controller in the school or college.
- The purpose in processing the data.
- Any third party to whom the biometric data will be given.

It is essential that students are aware of the purpose for which the biometrics data will be processed. This means that a school or college must carefully think through any purpose or potential purpose. Is the system solely for attendance management purposes? Will it be used for access control? What are the consequences for the student concerned if

there is an identified abuse of the system? Under what circumstances will management access logs created by the system?

Transparency is even more important where the biometric system does not require the knowledge or active participation of a student. A facial recognition system, for instance, may capture and compare images without that person's knowledge.

5. Accuracy

Section 2(1)(b) of the Acts require that data shall be: "Accurate and complete and, where necessary, kept up to date."

Any biometric system must accurately identify the persons whose data are processed by the system. If changes in physical or physiological characteristics result in a template becoming outdated, a procedure must be in place to ensure that the data are kept up to date.

6. Security

The requirement, under section 2(1)(d), that a school or college has appropriate security measures in place to prevent the unauthorised access to, or the unauthorised alteration, disclosure or destruction of data would appear to promote the use of technological solutions such as encryption.

However, in deciding upon what constitutes an appropriate security measure, Section 2C details four factors that should be taken into account:

- The state of technological development.
- The cost of implementing such technology.
- The nature of the data being protected.
- The harm that might result through the unlawful processing of such data.

A minimum standard of security would include:

- Access to the information restricted to authorised staff on a 'need to know' basis in accordance with a defined policy.
- Computer systems should be password protected.
- Information on computer screens or manual files should be hidden from persons who are not authorised to see them.
- A back-up procedure for computer held data, including off-site back-up.
- Ensuring that staff are made aware of the school or college's security measures, and comply with them.
- Careful disposal of documents such as computer printouts, etc.
- The designation of a person with responsibility for security and the periodic review of the security measures and practices in place.
- Adequate overall security of the premises when it is unoccupied.
- Where the processing of personal data is carried out by a data processor on behalf of the school or college, a contract should be in place which imposes equivalent security obligations on the data processor.

7. Retention

Section 2(1)(c)(iv) of the Data Protection Acts provides that data shall not be kept for longer than is necessary for the purpose. In the context of a biometric system in a school or college, it would be necessary to devise a retention policy in advance of the deployment of the system which clearly sets out the retention period which would apply to biometric data. At a minimum, the Data Protection Commissioner would expect that as soon as a student permanently leaves the school or college, his/her biometric data would be immediately deleted. Furthermore, in formulating a retention policy, the institution concerned should consider whether the biometric data of students should be deleted on a frequent basis while the students remain enrolled, for example, at the end of each school term or school year. In order to be able to support or justify their retention policy on biometrics, schools and colleges must ask themselves if they need to keep the information for a full term or full school year and be able to stand over the policy position they adopt.

8. Privacy Impact Assessment.

The Data Protection Commissioner cannot give a general approval or condemnation of biometric systems. Each system must be judged in respect of the situation in which it is used. A case-by-case judgement is required. With that in mind, the Commissioner encourages schools and colleges to take the above guidance into account if considering introducing any biometric system.

Before a school or college installs a biometric system, the Data Protection Commissioner recommends that a documented privacy impact assessment is carried out. A school or college which properly conducts such an assessment is less likely to introduce a system that contravenes the provisions of the Data Protection Acts 1988 & 2003. This is an important procedure to adopt as a contravention may result in action being taking against a school or college by the Commissioner, or may expose a school or college to a claim for damages from a student. Data protection responsibility and liability rests with the school or college, not with the person who has supplied the system (except where that person also acts as a data processor on behalf of the school or college).

Some of the points that might be included in a Privacy Impact Assessment are:

- Do I have an attendance management and/or access control system in place?
- Why do I feel I need to replace it?
- What problems are there with the system?
- Are these problems a result of poor administration of the system or an inherent design problem?
- Have I examined a number of types of system that are available?
- Will the non-biometric systems perform the required tasks adequately?
- Do I need a biometric system?
- If so, which kind do I need?
- Do I need a system that identifies students as opposed to a verification system?
- Do I need a central database?
- If so, what is wrong with a system that does not use a central database?
- What is the biometric system required to achieve for me?

- Is it for attendance management purposes and/or for access control purposes?
- How accurate shall the data be?
- What procedures are used to ensure accuracy of data?
- Will the data require updating?
- How will the information on it be secured?
- Who shall have access to the data or to logs?
- Why, when and how shall such access be permitted?
- What constitutes an abuse of the system by a student?
- What procedures shall I put in place to deal with abuse?
- What legal basis do I have for requiring students to participate?
- How will I obtain the consent of the existing students (or their parents/guardians if applicable)?
- How will I obtain the consent of new students (or their parents/guardians) who will enrol at a future date?
- How will I ensure that students will be given a clear and unambiguous right to opt out of a biometric system without penalty?
- What procedures will I put in place to provide for the withdrawal by students of consent previously given?
- What system will I put in place for students who opt out of using the biometric system?
- How will I ensure that students who are unable to provide biometric data, because of a disability for example, are not discriminated against by my school or college by being required to operate a different system, or otherwise?
- Does the system used employ additional identifiers (e.g. PIN number, smart card) along with the biometric?
- If so, would these additional identifiers be sufficient on their own, rather than requiring operation in conjunction with a biometric?
- What is my retention policy on biometric data?
- Can I justify the retention period in my retention policy?
- How shall I inform students about the system?
- What information about the system need I provide to students?
- Would I be happy if I was a student asked to use such a system?
- Am I happy to operate a biometric system in an educational establishment where the use of such a system can make students less aware of the data protection risks that may impact upon them in later life?
- Does my school or college have a comprehensive data protection policy as required by the Department of Education and Science since 2003?
- Have I updated this policy to take account of the introduction of a biometric system for use by students?

Guidance Note for Data Controllers on the Release of Personal Data To Public Representatives

Introduction

This Office recognises that it is a normal and accepted function of an Irish public representative to represent individual constituents in their dealings with public and private organisations. Such representations typically relate to access to services or to information about those services.

The following guidance note has been prepared as an aid to organisations ("data controllers") that are in receipt of representations made on behalf of individuals ("data subjects") by public representatives (TDs, Senators, MEPs, Councillors). This note also sets out the obligations on public representatives under the Data Protection Acts 1988 and 2003 in relation to the making of such representations for personal information and their responsibilities in relation to information which may come into their possession on foot of these representations.

Data Controllers

We advise that, where a public representative makes a written representation on behalf of a constituent, the organisation can generally assume that the constituent has given consent for the release of personal data necessary to respond to the representation.

As the organisation is accountable for personal data it has chosen to release, it should be satisfied that it is reasonable to assume that the individual whose personal data is being released would have no objection to such release through a public representative. In most cases, this is unlikely to be an issue. This would be true, for example, in relation to the many representations on behalf of individuals who simply wish to know when a particular service will be provided.

However, there will be cases where it would be appropriate for the organisation to check with the public representative, or the individual whose personal data is being released, that such release is not going to give rise to later complaints about breach of the Data Protection Acts.

This could arise, for example, where the constituent is making enquiries about the provision of services to a relative of the constituent where it is not clear that the relative supports, or is even aware of, the representation being made. Another example would be where access is being sought to information which would involve disclosure of personal data in relation to others (e.g. it would be wrong to release the names of the top ten individuals on a waiting list without their consent). Yet another example might be where the representation is being made in a context where the constituent is involved in a dispute with third parties. Particular care is needed where the information being released qualifies as "sensitive data" under the Data Protection Acts (e.g. information about the health of an individual).

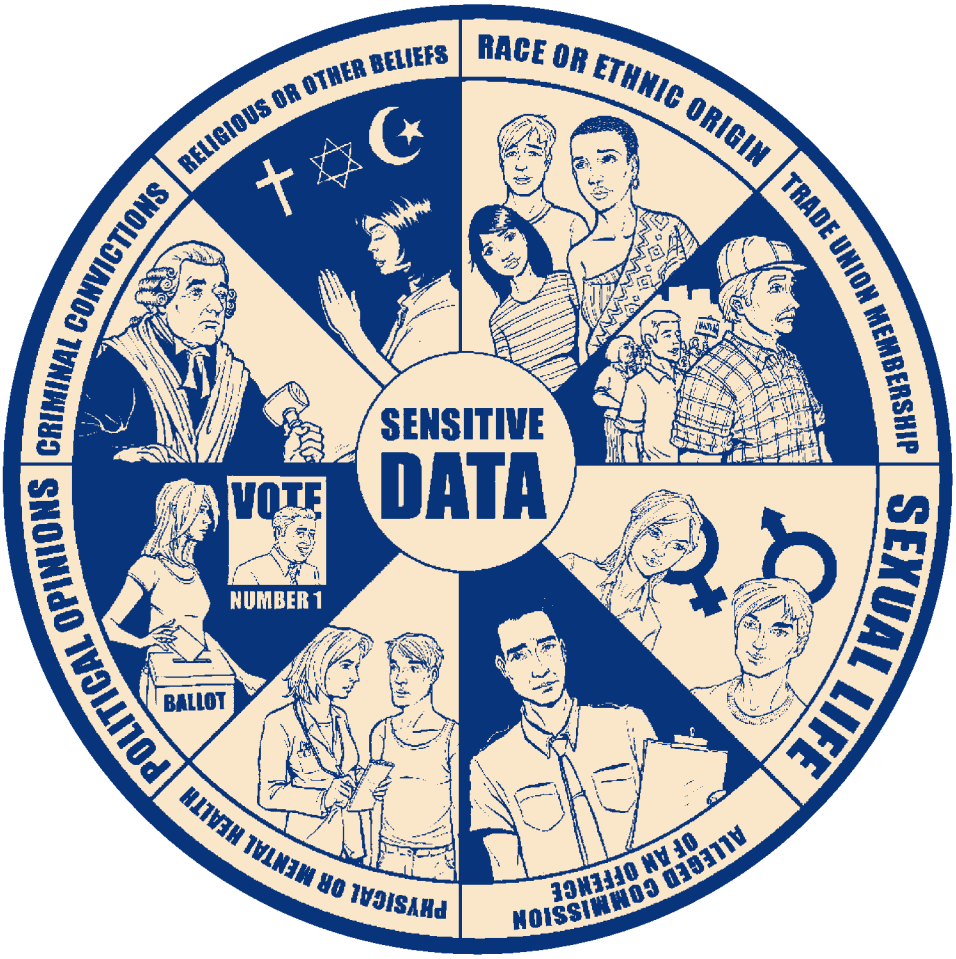
Public Representatives

Public representatives should also be aware of their obligations under the Data Protection Acts. They need to be satisfied that they are acting with the consent of the individual where the response to a representation involves release of that individual's personal data. They should also understand the obligations on organisations to keep personal data confidential and that, in particular cases, this may involve a need to check that the individual concerned has consented to the release of their personal data. When information has been supplied in reply to such representations, the public representative must act in compliance with Section 2 of the Acts which requires data controllers (in this case, public representatives) to comply with certain provisions regarding personal data kept by them:

- the data should not be further processed in a manner incompatible with the purpose for which it was received
- the data should be kept safe and secure while in the possession of the public representative
- the data should not be kept for longer than is necessary

SENSITIVE DATA

The catagories of data featured in the wheel diargram receive extra protection under the Data Protection Acts. Data Controllers must be able to justify why they need this data and they must take extra care when processing this data.



APPENDICES

Appendix 1 – Presentations

Appendix 2 – Registration Statistics

Appendix 3 – Account of Income and Expenditure

APPENDIX 1
PRESENTATIONS AND TALKS

During 2007 my Office staff and I gave presentations to the following organisations:

Citizens' Advice

Citizens' Information Blanchardstown
Citizens' Information Dublin
Citizens' Information Limerick
Citizens' Information Kilkenny

Educational

Coláiste Íosagáin, Portarlington
Coláiste Naomh Cormac
Mountmellick Community School
Patrician College, Ballyfin
Rathangan Secondary School
St Mary's Secondary School, Edenderry
St Patrick's College, Drumcondra
Msc in Health Informatics - Trinity College
Resources in Medical History - UCD School of History and Archives
Ard Scoil Chiaráin Naofa, Clara
3rd Level Colleges/Universities FOI Network
56th International Session of the European Youth Parliament
Visiting Teacher Service for Travellers
Irish Computer Society Data Protection Course

Financial Services

Card Not Present Fraud Prevention Task Force
Irish League of Credit Unions South East Area
Irish Institute of Credit Management Conference on Consumer Credit
IBF/ISP Hi-Tech Crime Forum

Government

CMOD FOI Course
Department of Foreign Affairs
Conference on Access to Public Sector Information
Heads of Administration of Civil Service Departments
Data Protection in the Public Sector organised by Public Affairs Ireland (x2)
IPA Certificate in Civil Service & State Agency Studies

Health Sector

Beaumont Hospital
Department of General Practice Clinical Science Institute Lunchtime Seminar
Health Service Executive – Healthcare Risk Manager's Forum
Launch of National Hospital's Office Code of Practice on Records Management

Insurance Sector

The Insurance Institute of Ireland (x3)

International

Singapore Civil Service College
US-EU Conference on Safe Harbour - Washington
Data Protection Compliance Conference - Brussels
Consultative Conference on Data Sharing guidelines - Belfast
International Association of Privacy Professionals- Washington & San Francisco
OECD Conference on the Participative Web - Ottawa

Legal Sector

Legal Aid Board
The Council of the Bar of Ireland

Local Authorities

Homeless Agency

Mixed Seminars

Association for Information and
Image Management (x2)
Data Protection Compliance organised by IIR (x2)
BH Consulting-Global Security Week
Business and Professional Women Galway
Data Security Briefing organised by the Calyx Group
Information Systems Audit and Control Association
Data Protection Practical Compliance Conference, Privacy and Data Protection
Data Protection Compliance Conference organised by Privacy and Data Protection Ireland
IT Security Conference organised by Entropy
Data Protection Compliance Briefing organised by Data Solutions Ltd.

Records Management

The Records Management Society

Voluntary/Charity

West Training and Development Limited

APPENDIX 2
REGISTRATIONS
2005 / 2006 / 2007

(a) Public authorities and other bodies and persons referred to in the Third Schedule

	2005	2006	2007
Civil service Departments/Offices	147	170	154
Local Authorities & VECs	160	167	171
Health Boards/Public Hospitals	60	57	32
Commercial State Sponsored Bodies	45	40	25
Non-Commercial & Regulatory	178	170	152
Third level	56	55	48
Sub-total	646	659	582

(b) Financial institutions, insurance & assurance organisations, persons whose business consists wholly or mainly in direct marketing, providing credit references or collecting debts.

Associated Banks	45	55	47
Non-associated banks	72	74	84
Building societies	7	7	9
Insurance & related services	342	414	437
Credit Union & Friendly Societies	440	439	402
Credit Reference/ Debt Collection	41	41	42
Direct Marketing	69	68	64
Sub-total	1016	1098	1085

(c) Any other data controller who keeps sensitive personal data

	2005	2006	2007
Primary & secondary schools	622	647	329
Miscellaneous commercial	176	203	228
Private hospitals/health	149	155	156
Doctors, dentists, health professionals	850	926	959
Pharmacists	867	950	987
Political parties & public representatives	162	166	119
Religious, voluntary & cultural organisations	186	213	176
Legal Profession	629	636	435
Sub-total	3641	3896	3389

(d) Data processors	603	696	579

(e) those required under S.I. 2/2001			
Telecommunications / Internet Access providers	27	31	64
TOTAL	5933	6380	5699

In 2007 the number of organisations registered decreased by 681 or 10.7%. The decrease is a result of the implementation of the new registration regulations (S.I. No. 657 of 2007) after 1st October 2007. Changes in the requirement to register in the education and legal profession sectors contributed most to the decrease.

APPENDIX 3

Office of the Data Protection Commissioner – Abstract* of Receipts and Payments in the year ended 31 December 2007

	2006	2007
	€	€
Receipts		
Moneys provided by the Oireachtas	1,281,521	1,835,375
Registration Fees	586,817	535,405
	1,868,338	2,370,780
Payments		
Staff Costs	1,020,822	1,297,809
Establishment Costs	178,183	269,940
Education and Awareness	59,822	158,587
Legal and Professional Fees	4,695	59,473
Incidental and Miscellaneous	17,999	49,566
	1,281,521	1,835,375
Payments of Fees to the Vote for the Office of the Minister of Justice, Equality and Law Reform	586,817	535,405
	1,868,338	2,370,780

**The financial statements of the Office are subject to audit by the Comptroller and Auditor General and after audit are presented to the Minister for Justice, Equality and Law Reform for presentation to the Oireachtas.*